

ORIGINAL

1 CAROLINE WILSON PALOW (SBN 241031)
2 caroline@privacyinternational.org
3 SCARLET KIM
4 scarlet@privacyinternational.org
5 PRIVACY INTERNATIONAL
6 62 Britton Street
7 London EC1M 5UY
8 United Kingdom
9 Telephone: +44.20.3422.4321

FILED
CLERK, U.S. DISTRICT COURT
MAR - 3 2016
CENTRAL DISTRICT OF CALIFORNIA
EASTERN DIVISION BY DEPUTY

LOGGED

2016 MAR 13 PM 1:19
CLERK U.S. DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA
BY

10 Attorneys for *Amici Curiae*
11 PRIVACY INTERNATIONAL
12 HUMAN RIGHTS WATCH

13 UNITED STATES DISTRICT COURT
14 CENTRAL DISTRICT OF CALIFORNIA
15 EASTERN DIVISION

16 IN THE MATTER OF THE SEARCH) ED No. CM 16-10 (SP)
17 OF AN APPLE IPHONE SEIZED)
18 DURING THE EXECUTION OF A) ~~PROPOSED~~ ORDER GRANTING
19 SEARCH WARRANT ON A BLACK) LEAVE TO FILE BRIEF OF AMICI
20 LEXUS IS300, CALIFORNIA) CURIAE PRIVACY
21 LICENSE PLATE 35KGD203) INTERNATIONAL AND HUMAN
22) RIGHTS WATCH
23)
24) **Hearing:**
25) Date: March 22, 2016
26) Time: 1:00 p.m.
27) Place: Courtroom 3 or 4
28) Judge: Hon. Sheri Pym

1. On March 3, 2016, Privacy International and Human Rights Watch (“HRW”) filed an application for leave to file an *amicus curiae* brief in the above-captioned matter.

1
2
3
4 2. Having considered the arguments and authorities offered by Privacy
5 International and HRW, and good cause appearing therefore, the Court grants the
6 application and deems filed the brief submitted with the application.
7

8 IT IS SO ORDERED.
9

10 Dated: March 3, 2016
11
12
13

14 
15 _____
16 HON. SHERI PYM
17 United States Magistrate Judge
18
19
20
21
22
23
24
25
26
27
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

PROOF OF SERVICE

I am a citizen of the United States of America and employed in London, the United Kingdom. I am over the age of 18 and not a party to the within action. My business address is Privacy International, 62 Britton Street, London EC1M 5UY, United Kingdom.

On March 3, 2016, I caused to be served through mail (FedEx) and/or e-mail on each person on the attached Service List the foregoing document described as:

[PROPOSED] ORDER GRANTING LEAVE TO FILE BRIEF OF AMICI CURIAE PRIVACY INTERNATIONAL AND HUMAN RIGHTS WATCH

Service List


Service Type	Counsel Served	Party
E-mail*	Theodore J. Boutrous, Jr. Nicola T. Hanna Eric D. Vandavelde Gibson, Dunn & Crutcher LLP 333 South Grand Avenue Los Angeles, CA 90071-3197 Telephone: (213) 229-7000 Facsimile: (213) 229-7520 Email: tboutrous@gibsondunn.com nhanna@gibsondunn.com evandavelde@gibsondunn.com	Apple, Inc.
E-mail*	Theodore B. Olson Gibson, Dunn & Crutcher LLP 1050 Connecticut Avenue, N.W. Washington, D.C. 20036-5306 Telephone: (202) 955-8500 Facsimile: (202) 467-0539 Email: tolson@gibsondunn.com	Apple, Inc.
E-mail*	Marc J. Zwillinger Jeffrey G. Landis Zwillgen PLLC	Apple, Inc.

	1900 M Street N.W., Suite 250 Washington, D.C. 20036 Telephone: (202) 706-5202 Facsimile: (202) 706-5298 Email: marc@zwillgen.com jeff@zwillgen.com	
Mail & E-mail	Eileen M. Decker Patricia A. Donahue Tracy L. Wilkison Allen W. Chui 1500 United States Courthouse 7312 North Spring Street Los Angeles, California 90012 Telephone: (213) 894-0622/2435 Facsimile: (213) 894-8601-7520 Email: Tracy.Wilkison@usdoj.gov Allen.Chiu@usdoj.gov	United States of America

*Apple, Inc. has consented in writing to service by electronic means in accordance with Federal Rule of Civil Procedure 5(b)(E), Local Civil Rule 5-3.1.1, and Local Criminal Rule 49-1.3.2(b).

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct and that I have made service at the direction of a member of the bar of this Court.

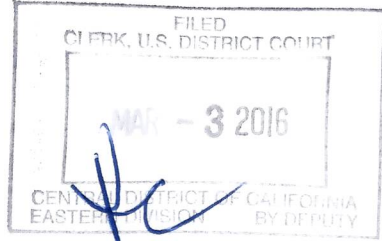
Executed on March 3, 2016 in London, United Kingdom



Sara Nelson

ORIGINAL

CAROLINE WILSON PALOW (SBN 241031)
caroline@privacyinternational.org
SCARLET KIM
scarlet@privacyinternational.org
PRIVACY INTERNATIONAL
62 Britton Street
London EC1M 5UY
United Kingdom
Telephone: +44.20.3422.4321



Attorneys for *Amici Curiae*
PRIVACY INTERNATIONAL
HUMAN RIGHTS WATCH

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA
EASTERN DIVISION

IN THE MATTER OF THE SEARCH) ED No. CM 16-10 (SP)
OF AN APPLE IPHONE SEIZED)
DURING THE EXECUTION OF A) **BRIEF OF AMICI CURIAE**
SEARCH WARRANT ON A BLACK) **PRIVACY INTERNATIONAL AND**
LEXUS IS300, CALIFORNIA) **HUMAN RIGHTS WATCH**
LICENSE PLATE 35KGD203)
) **Hearing:**
) Date: March 22, 2016
) Time: 1:00 p.m.
) Place: Courtroom 3 or 4
) Judge: Hon. Sheri Pym

LOGGED

FILED MAR -3 PM 1:49
CLERK U.S. DISTRICT COURT
CENTRAL DIST. OF CALIF.
RIVERSIDE

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

TABLE OF CONTENTS

I. INTRODUCTION 1

II. INTERESTS OF *AMICI CURIAE* 2

III. BACKGROUND 3

 A. The iPhone and its Passcode 3

 B. Procedural History 4

IV. ARGUMENT 6

 A. The Order Sets a Far-reaching Precedent that the Government May
 Compel Technology Companies to Undermine the Security of their Products
 and Services 6

 B. Compelling Technology Companies to Undermine the Security of their
 Products and Services Threatens the Security of the Internet 8

 C. The Order Signals to Other Countries that it is Permissible and
 Appropriate to Compel Technology Companies to Undermine the Security of
 their Products and Services 12

 D. Other Countries Will Compel Technology Companies to Undermine the
 Security of their Products and Services In Order to Commit Civil and Human
 Rights Abuses 19

V. CONCLUSION 22

TABLE OF AUTHORITIES

OTHER AUTHORITIES

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Alice Truong, *What Chinese slowdown? Apple’s sales double in China on iPhone growth*, Quartz (Oct. 27, 2015) -----19

Andrea Peterson, *Forbes Web site was compromised by Chinese cyberespionage group, researchers say*, Wash. Post (Feb. 10, 2015)-----10

Ankit Panda, *Beijing Strikes Back in US-China Tech Wars*, The Diplomat (Mar. 6, 2015) -----18

Apple Inc. and Apple Dist. Int’l, *Written Evidence to the UK Parliament Joint Comm. on the Draft Investigatory Powers Bill (IPB0093)* (Jan. 7, 2016)14, 15, 16

Apple Inc., *iOS Security: iOS 9.0 or later* (Sept. 2015) ----- 4

Ben Elgin, Vernon Silver & Alan Katz, *Iranian Police Seizing Dissidents Get Aid of Western Companies*, Bloomberg (Oct. 31, 2011) -----21

Bruce Schneier, *Data and Goliath* (2015)-----10

Council of Europe, European Commission for Democracy through Law, *Opinion on the Federal Law on the Federal Security Service (FSB) of the Russian Federation* (2012) -----14

Dep’t of Homeland Security, *Mobile Security Tip Card*-----12

Ellen Nakashima, *Meet the woman in charge of the FBI’s most controversial high-tech tools*, Wash. Post (Dec. 8, 2015)-----9, 11

Eva Galperin, *Don’t get your sources in Syria killed*, Committee to Protect Journalists (May 21, 2012) -----21

Facebook Inc., Google Inc., Microsoft Corp., Twitter Inc. and Yahoo Inc., *Written Evidence to the UK Parliamentary Joint Comm. on the Draft Investigatory Powers Bill (IPB0116)* (Jan. 7, 2016)-----15

Federal Law of the Russian Federation on the Federal Security Service Act (no. 40-FZ) 1995 -----13

1 Human Rights Watch, *China: Draft Counterterrorism Law a Recipe for Abuses*
 2 (Jan. 20, 2015) ----- 17

3 Human Rights Watch, *Submission by HRW to the National People’s Congress*
 4 *Standing Committee on the draft Cybersecurity Law* (Aug. 4, 2015) ----- 19

5 Turkey Information and Communication Technologies Authority, *By Law on the*
 6 *Procedures and Principles of Encoded or Encrypted Communication between*
 7 *Public Authorities and Organizations and Real and Legal Persons in Electronical*
 8 *[sic] Communication Service* (Oct. 23, 2010) ----- 17

9 Investigatory Powers Bill 2015-16, Bill [143] (Gr. Brit.) ----- 14, 15

10 Jeff Mason, *Exclusive: Obama sharply criticizes China’s plans for new technology*
 11 *rules*, Reuters (Mar. 2, 2015)----- 18

12 Kadhim Shubber, *BlackBerry gives Indian government ability to intercept*
 13 *messages*, Wired (July 11, 2013) ----- 16

14 Katie Collins, *BlackBerry to leave Pakistan after refusing to ditch user privacy*,
 15 CNET (Dec. 1, 2015)----- 16

16 Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware*
 17 *Attack*, Wired (Sept. 13, 2013)----- 9, 10

18 Lance Whitney, *RIM averts BlackBerry ban in UAE*, CNET (Oct. 8, 2010) ----- 17

19 Law Library of Congress, *Russian Federation Translation of National Legislation*
 20 *into English* (March 2012)----- 13

21 Letter to Court, *In re Order Requiring Apple, Inc. to Assist in the Execution of a*
 22 *Search Warrant Issued by this Court*, No. 15-MC-1902 (E.D.N.Y. Feb. 17,
 23 2016), Dkt. 27 ----- 12

24 Martin Kaste, *Slippery Slope? Court Orders Apple to Unlock Shooter’s iPhone*,
 25 NPR (Feb. 18, 2016) ----- 12

26 Noah Shachtman, *Russia’s Top Cyber Sleuth Foils US Spies, Helps Kremlin Pals*,
 27 Wired (July 23, 2012) ----- 13

28 Patrick Howell O’Neill, *How cybercriminals use major news events to attack you*,
 The Daily Dot (Aug. 5, 2013)----- 9

1 President’s Review Group on Intelligence and Communications Technologies,
 2 *Liberty and Security in a Changing World* (Dec. 12, 2013) ----- 11

3 *Provisions of China’s counterterrorism bill inspired by foreign laws: official,*
 4 *Xinhua* (Dec. 27, 2015) ----- 19

5 *Report of the Special Rapporteur on the promotion and protection of human rights*
 6 *and fundamental freedoms while countering terrorism, Martin Scheinin,*
 7 *delivered to the Human Rights Council, U.N. Doc. A/HRC/13/37* (Dec. 28, 2009)
 ----- 19

8 *Report of the Special Rapporteur on the promotion and protection of the right to*
 9 *freedom of opinion and expression, David Kaye, delivered to the Human Rights*
 10 *Council, U.N. Doc. A/HRC/29/32, (May 22, 2015) ----- 17, 18, 20*

11 *Report of the Special Rapporteur on the promotion and protection of the right to*
 12 *freedom of opinion and expression, Frank La Rue, delivered to the Human Rights*
 13 *Council, U.N. Doc. A/HRC/23/40* (Apr. 23, 2013) ----- 19

14 *RIM to share some BlackBerry codes with Saudis, Reuters* (Aug. 10, 2010)----- 17

15 *Samm Sacks, Apple in China, Part I: What Does Beijing Actually Ask of*
 16 *Technology Companies?, Lawfare* (Feb. 22, 2016) ----- 18

17 *The Right to Privacy in the Digital Age, G.A. Res. 69/166, pmbl., U.N. Doc.*
 18 *A/Res/69/166* (Feb. 10, 2014)----- 21

19 *Tom Mitchell, Obama seeks reboot of China cyber laws, Fin. Times* (Mar. 3, 2015)
 20 ----- 17

21 *U.S. Submission to the Special Rapporteur on the Promotion of the Right to*
 22 *Freedom of Opinion and Expression* (Feb. 26, 2015)----- 20, 21

23 *Vernon Silver & Ben Elgin, Torture in Bahrain Becomes Routine With Help From*
 24 *Nokia Siemens, Bloomberg* (Aug. 22, 2011)----- 21

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

Compelling Apple, Inc. (“Apple”) to remove security features from its iPhone will have global and wide-ranging implications. It is for this reason that Privacy International and Human Rights Watch (“HRW”) submit this *amicus curiae* brief. Both organizations have spent years monitoring and critiquing the surveillance practices and human rights records of governments worldwide. This matter sits at an important crossroads that has arisen in that space. The path the United States takes will impact how other governments will approach the increasing tension between their desire for ready access to electronic data and the need for robust security features that allow us to communicate, express ourselves, and assert our fundamental rights in a digital age. If the Order stands, governments around the world may view it as encouragement to preference the former by similarly requiring technology companies to undermine the security of their products and services. Many countries are already considering such powers.

The mere existence of the power the government seeks may erode the security infrastructure of the Internet. If Apple can be compelled to undermine its security features, what confidence can users of Apple and other technology products and services actually place in those features? For instance, would it be appropriate to trust a software security update from a company that could be compelled to include malicious software – often called malware – in that update?¹ Yet these security updates are crucial to protecting all of our data and devices, since they are normally deployed to fix vulnerabilities that might otherwise be exploited by hackers, including criminals and foreign agents.²

¹ “Malware” refers to any software that performs unwanted tasks, typically for the benefit of a third party. Malware can range from a simple irritant to a serious breach of privacy (e.g. stealing data from a computer).

² “Hacking” can refer to several different activities. In computing terms, it originally described the hobby of computer programming and encompassed the idea of finding creative solutions to technology problems. The term gradually evolved to describe the activity of finding

1 Security features – including encryption and other measures – are integral to
2 the protection of civil and human rights. Countries may seek to compel technology
3 companies to impair security for illegitimate purposes, including to stifle
4 expression, crush dissent, and facilitate arbitrary arrest and torture. In these
5 societies, secure technologies protect all members of society but especially
6 vulnerable ones – such as journalists, human rights defenders, and political
7 activists – by giving them a safe space to communicate, research, and organize.
8 The U.S., by compelling technology companies to roll back these protections, risks
9 exposing the millions of individuals who reside and work in these places to abuse
10 by their governments.

11 For all of these reasons, Privacy International and HRW strongly urge the
12 Court to consider the wider implications of the Order compelling Apple to assist in
13 the search of the iPhone at issue. They hope this submission will help the Court in
14 making the difficult decision it faces.

15 II. INTERESTS OF *AMICI CURIAE*

16 Privacy International is a nonprofit, nongovernmental organization based in
17 London dedicated to defending the right to privacy around the world. Established
18 in 1990, Privacy International undertakes research and investigations into state and
19 corporate surveillance with a focus on the technologies that enable these practices.
20 It has litigated or intervened in cases implicating the right to privacy in the courts
21 of the US, the United Kingdom (“U.K.”) and Europe, including the European
22 Court of Human Rights. To ensure universal respect for the right to privacy,
23 Privacy International advocates for strong national, regional and international laws
24

25
26 vulnerabilities in computer security, first with the goal of reporting or repairing them (“white
27 hat”), but later to exploit them (“black hat”). The black hat iteration of hacking is the mainstream
28 usage of the term and is the definition adopted throughout this brief. That definition encompasses
the activity of any attacker – including criminals and foreign agents – seeking to exploit a
vulnerability in computer security.

1 that protect privacy. It also strengthens the capacity of partner organizations in
2 developing countries to do the same.

3 Human Rights Watch (“HRW”) has been reporting on abuses connected to
4 the practice of state surveillance since its inception more than three decades ago as
5 Helsinki Watch, with particular focus on mass surveillance practices since 2013.
6 HRW’s reports detail abuses of rights connected to surveillance around the globe
7 (for example, in China, Ethiopia, Saudi Arabia, and the U.S.), and its advocacy
8 involves legal analysis and submissions on the various legal authorities (actual or
9 proposed) for surveillance practices to the relevant bodies of the United Nations
10 (“U.N.”), the U.S., the U.K., the UN High Commissioner for Human Rights, the
11 Special Rapporteur for Freedom of Expression, as well as comment and analysis
12 on the laws of many other countries in respect of these issues.

13 III. BACKGROUND

14 A. The iPhone and its Passcode

15 The device at the heart of this dispute is an iPhone 5c running operating
16 system (“iOS”) 9. *Ex Parte* Application for Order Compelling Apple Inc. to Assist
17 Agents in Search, *In the Matter of the Search of an Apple iPhone Seized during the*
18 *Execution of a Search Warrant on a Black Lexus IS300, California License Plate*
19 *35KGD203 (“Apple iPhone”),* ED No. 15-0451M *1, *4 (C.D. Cal. Feb. 16, 2016)
20 [hereinafter “*Ex Parte* Application”]. In September 2014, Apple announced that
21 “iPhones . . . operating Apple’s then-newest operating system, iOS 8, would
22 include hardware-and software-based encryption of the password-protected
23 contents of the devices by default.” Declaration of Erik Neuenschwander in
24 Support of Apple’s Motion to Vacate, *Apple iPhone*, ED No. 15-0451M, ¶ 8 (C.D.
25 Cal. Feb. 16, 2016), Dkt. 16, attach. 33 [hereinafter “*Neuenschwander Decl.*”].
26 What this development meant was that individuals with an iPhone running iOS 8
27 or newer operating systems could, by setting up a passcode, enable encryption of
28 their iPhone data. *Id.* at ¶ 9; *see also* Declaration of Caroline Wilson Palow in

1 support of Brief of *Amici Curiae* Privacy International and Human Rights Watch
2 [hereinafter “Palow Decl.”], Ex. A, at 12 [Apple Inc., *iOS Security: iOS 9.0 or*
3 *later* (Sept. 2015) [hereinafter “*iOS Security I*”]. The data on the device cannot be
4 decrypted without the correct cryptographic key, and this key is protected by a key
5 derived from the user-chosen passcode. Palow Decl. Ex. A at 12 [*iOS Security*]. In
6 short, “[t]he end result is a person must know that passcode to read [the iPhone’s]
7 data.” Dkt. 16, attach. 33 ¶ 9 [Neuenschwander Decl.].

8 Apple has devised a number of safeguards to protect against “brute-force”
9 attempts to determine the passcode. First, Apple uses a “large iteration count”,
10 which “functions to slow attempts to unlock an iPhone”. *Id.* at ¶ 11. The iteration
11 count is “calibrated so that . . . it would take more than 5 ½ years to try all
12 combinations of a six-character alphanumeric passcode with lowercase letters and
13 numbers.” Palow Decl. Ex. A at 12 [*iOS Security*]. Second, Apple imposes
14 escalating time delays after each entry of an invalid passcode. *Id.*; Dkt. 16, attach.
15 33 ¶ 12 [Neuenschwander Decl.]. Finally, an individual can turn on the “Erase
16 Data” setting, which automatically wipes the keys needed to read the encrypted
17 data after ten consecutive incorrect attempts to enter the passcode. Dkt. 16, attach.
18 33 ¶ 12 [Neuenschwander Decl.]; Palow Decl. Ex. A at 12 [*iOS Security*].

19 **B. Procedural History**

20 On February 16, 2016, the government filed an *ex parte* application in this
21 Court for an order pursuant to the All Writs Act, 28 U.S.C. § 1651, compelling
22 Apple to “provide assistance to agents of the Federal Bureau of Investigation
23 (“FBI”) in their search of a cellular telephone.” *Ex Parte* Application, at *1. That
24 same day, this Court issued an order compelling Apple to provide “reasonable
25 technical assistance to law enforcement agents in obtaining access to the data on
26 the SUBJECT DEVICE.” Order Compelling Apple, Inc. to Assist Agents in
27 Search, *Apple iPhone*, ED No. 15-0451M, *2 (C.D. Cal. Feb. 16, 2016)
28 [hereinafter “Order”]. The Order specified that

1 Apple's reasonable technical assistance shall accomplish the following
2 three important functions: (1) it will bypass or disable the auto-erase
3 function whether or not it has been enabled; (2) it will enable the FBI to
4 submit passcodes to the SUBJECT DEVICE for testing electronically
5 via the physical device port, Bluetooth, Wi-Fi, or other protocol
6 available on the SUBJECT DEVICE; and (3) it will ensure that when
7 the FBI submits passcodes to the SUBJECT DEVICE, software running
8 on the device will not purposefully introduce any additional delay
9 between passcode attempts beyond what is incurred by Apple
10 hardware.

11 *Id.* at *2.

12 On February 16, 2016, Apple informed the government and this Court that it
13 would seek relief from the Order. Scheduling Order, *Apple iPhone*, ED No. CM
14 16-10 ¶ 1 (C.D. Cal. Feb. 16, 2016), Dkt. 9 [hereinafter "Scheduling Order"]. On
15 February 19, 2016, the government filed a motion to compel Apple to comply with
16 the Order. Government's Motion to Compel Apple, Inc. to Comply with this
17 Court's February 16, 2016 Order Compelling Assistance in Search, *Apple iPhone*,
18 ED No. CM 16-10 (C.D. Cal. Feb. 19, 2016), Dkt. 1 [hereinafter "Motion to
19 Compel"]. That day, this Court issued a Scheduling Order setting a briefing
20 schedule for Apple's application for relief, which instructed that "[a]ny amicus
21 brief shall be filed by not later than March 3, 2016, along with an appropriate
22 request seeking leave of the Court to file such brief." Dkt. 9, at ¶ 4(ii) [Scheduling
23 Order]. On February 26, 2016, Apple filed its application for relief and opposition
24 to the government's Motion to Compel. Apple Inc.'s Motion to Vacate Order
25 Compelling Apple Inc. to Assist Agents in Search, and Opposition to
26 Government's Motion to Compel Assistance, *Apple iPhone*, Ed No. CM 16-10 *6
27 (C.D. Cal. Mar. 22, 2016), Dkt. 16 [hereinafter "Motion to Vacate"].
28

IV. ARGUMENT

A. The Order Sets a Far-reaching Precedent that the Government May Compel Technology Companies to Undermine the Security of their Products and Services

This Court's Order, by requiring Apple to develop new software to weaken the iPhone's passcode protection, establishes a precedent that the government may compel technology companies to undermine the security of their products and services. This dramatic expansion of the government's investigative authority is not limited to a single device manufactured by a single company. Rather, this new power could conceivably extend to any service or device – laptop, mobile phone, or the increasing number of other things connected to the Internet – provided by any company.

The government downplays the assistance it seeks from Apple, describing it as “providing the FBI with the opportunity to determine the passcode” to an iPhone. Dkt. 1 at *2 [Motion to Compel]. But the government's submissions critically overlook the *purpose* for which Apple would develop new software under the Order. That purpose is explicitly to weaken the security of one of its products. Apple designed the subject iPhone so that a user, by setting up a passcode, automatically enables encryption of her data. The cryptographic key to decrypt the data is protected by a key derived from the user's passcode. Thus, the passcode is essential to the decryption process and is therefore a critical element of the security of the iPhone.³ By compelling Apple to “modify” its operating system, the government is compelling it to “modify” a critical security feature of the iPhone.

Amici contend that this so-called “modification” is nothing short of hacking. In neutral terms, hacking is about exploring – often in creative fashion –

³ The government's assertion that it is asking Apple to “writ[e] a program that turns off non-encryption features” is not technically accurate. Dkt. 1 at *14 [Motion to Compel]. As explained above, the passcode is a fundamental part of the iPhone's encryption process and cannot therefore be objectively described as a “non-encryption feature”.

1 vulnerabilities in computer security. But it is only in its negative connotation that it
2 encompasses the activity of exploiting those vulnerabilities to deliberately
3 undermine security. That negative connotation of hacking is what the government
4 seeks to compel from Apple. It asks Apple to design and then create software that
5 purposefully creates cracks in the iPhone's security.

6 Although the government represents that "the Order is tailored for and
7 limited to this particular phone", Dkt. 1 at *14 [Motion to Compel], the legal
8 theory upon which it rests is unbounded. In simple terms, and in the government's
9 own words, the All Writs Act, 28 U.S.C. § 1651, compels "reasonable third-party
10 assistance that is necessary to exercise a warrant."⁴ Dkt. 1 at *7 [Motion to
11 Compel]. For the government, "reasonable" boils down to technical feasibility; its
12 overarching proposition is that "Apple retains . . . the technical ability to comply
13 with the Order, and so should be required to obey it." *Id.* at *1; *see also id.* at *13-
14 *14.

15 Technical feasibility is a meaningless constraint because, in technical terms,
16 many strategies for undermining the security of an iPhone may be feasible. As
17 Apple hypothesizes, if it
18 can be forced to write code in this case to bypass security features and
19 create new accessibility, what is to stop the government from
20 demanding that Apple write code to turn on the microphone in aid of
21 government surveillance, activate the video camera, surreptitiously
22
23

24 ⁴ Apple argues that the government's reading of the All Writs Act is unbounded for two reasons.
25 First, it recognizes no contextual limitation; any warrant in any investigation could provide the
26 basis for a supplemental All Writs Act Order to a third party. Dkt. 16 at *3 [Motion to Vacate].
27 Second, "under the government's formulation, any party whose assistance is deemed 'necessary'
28 by the government falls within the ambit of the All Writs Act and can be compelled to do
anything the government needs to effectuate a lawful court order." *Id.* at *25-*26. Privacy
International does not repeat those arguments here but focuses on the government's
interpretation of what is "reasonable third-party assistance" under the All Writs Act.

1 record conversations, or turn on location services to track the phone's
2 user?

3 Dkt. 16 at *4 [Motion to Vacate]; *see also id.* at *25-*26. Apple possesses the
4 technical capability to write and deploy such code.

5 If the government can compel Apple – because it is technically feasible – to
6 develop code to weaken iPhone security under the All Writs Act, it can compel any
7 other technology company to similarly sabotage its own devices. The proliferation
8 of Internet-connected devices – from computers to cars to refrigerators –
9 exponentially increases the ways the government could seek such assistance. And
10 the technology companies that could be conscripted into government service are
11 not limited to those that manufacture devices. Every day, more and more of our
12 lives are conducted in the digital realm. Equally, more and more of our physical
13 realm is governed and mediated by digital technologies. Many companies provide
14 services in both realms, from hosting websites to storing documents to transferring
15 money between bank accounts. Every one of these companies could conceivably
16 be compelled to develop software that weakens the security of these services and
17 the data, often precious to the individual to which it relates, that it stores.

18 **B. Compelling Technology Companies to Undermine the Security of their**
19 **Products and Services Threatens the Security of the Internet**

20 Compromising the security of a single technology product, like an iPhone,
21 can send negative ripple effects throughout the Internet. Those effects are
22 enhanced where what is compromised is a server or a network, to which hundreds
23 or thousands of people may connect. And the ramifications of compromising a
24 device, server or network are perilously amplified should the government seek to
25 regularly compel technology companies to undertake such activity.

1 A powerful example of how undermining a single service can breach the
2 security of many is a “watering hole” attack.⁵ This type of attack can target a
3 group, such as a business or organization, by identifying a website frequented by
4 its members and placing malware on it. *See* Palow Decl. Ex. B [Patrick Howell
5 O’Neill, *How cybercriminals use major news events to attack you*, The Daily Dot
6 (Aug. 5, 2013)] (defining a “watering hole” attack and describing common
7 iterations). The malware silently compromises the devices that visit the website, by
8 dropping additional malware onto those devices, which can allow the attacker to
9 access sensitive data or even control the affected devices. *See id.*

10 Under an All Writs Act order, the government could compel a web hosting
11 provider to implement a “watering hole” attack by developing and installing
12 custom code on a website (or multiple websites) that it operates. Indeed, the FBI
13 has already admitted to deploying such an attack itself. *See* Palow Decl. Ex. C
14 [Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware*
15 *Attack*, Wired (Sept. 13, 2013) [hereinafter *FBI Admits It Controlled Tor Servers*]].
16 An order under the All Writs Act would permit the FBI to instead compel a
17 company to carry out the attack, an alternative it is likely to prefer. *See* Palow
18 Decl. Ex. D [Ellen Nakashima, *Meet the woman in charge of the FBI’s most*
19 *controversial high-tech tools*, Wash. Post (Dec. 8, 2015) [hereinafter “*Meet the*
20 *woman*”]] (citing Amy Hess, executive assistant director for the FBI’s Science and
21 Technology Branch, as stating that “hacking computers is not a favored FBI

22 ⁵ Apple presents the security hazards inherent in developing new software to weaken the
23 iPhone’s passcode protection, even if it is only to be deployed on a single iPhone. Dkt. 16 at *13-
24 *14 [Motion to Vacate] (noting that the entire process “would need to be logged and recorded in
25 case Apple’s methodology is ever questioned, for example in court”); *id.* at *24-*25 (describing
26 the alternative to building and destroying software for each law enforcement demand as
27 “securing against disclosure or misappropriation” all physical and digital materials related to
28 such software); Dkt. 16, attach. 33 ¶¶ 39-43 [Neuenschwander Decl.] (indicating that it would be
“unrealistic” to “truly destroy the actual operating system and the underlying code”, which
remains “persistent”). Privacy International does not repeat those arguments here but focuses on
how undermining a technology service rather than a device can impact the security of the
Internet.

1 technique” because “[a]s soon as a tech firm updates its software, the tool
2 vanishes”).

3 A “watering hole” attack is particularly pernicious from a security
4 perspective because the attacker typically selects legitimate, trusted websites,
5 which may receive hundreds or thousands of daily visitors. A recent example of
6 such an attack occurred in November 2014, when Chinese hackers infected
7 Forbes.com as a way of targeting visitors working in the US defense and financial
8 services industries. *See* Palow Decl. Ex. E [Andrea Peterson, *Forbes Web site was*
9 *compromised by Chinese cyberespionage group, researchers say*, Wash. Post (Feb.
10 10, 2015) [hereinafter “*Forbes Web site was compromised*”]]. Moreover, even
11 where the attack targets a specific group of individuals, every visitor to the
12 compromised website is vulnerable to a security breach. In the FBI “watering hole”
13 attack cited above, the government compromised every site – and every visitor to
14 those sites – hosted by a particular server, some of which had no relation to the
15 government’s investigation. Palow Decl. Ex. C [*FBI Admits It Controlled Tor*
16 *Servers*].

17 The security of the Internet operates like a fragile ecosystem, where a
18 compromised device or service can negatively affect many other users. That
19 ecosystem is unlikely to survive should the government seek to regularly compel
20 technology companies to undermine the security of their products or services.⁶ In
21 the “watering hole” attack scenario, regular attacks would spell disaster, in part
22 because many “watering hole” attacks rely on what are called zero day
23 vulnerabilities. A zero day vulnerability refers to a security flaw in software that is
24 unknown to the vendor. *See* Palow Decl. Ex. F at 145-46 [Bruce Schneier, *Data*
25 *and Goliath* (2015)] (“Unpublished vulnerabilities are called ‘zero-day’
26 vulnerabilities; they’re very valuable to attackers because no one is protected

27
28 ⁶ Apple describes the security implications of repeated requests to weaken the passcode
protection on the iPhone. *See* Dkt. 16, attach. 33 ¶¶ 46-47 [Neuenschwander Decl.].

1 against them, and they can be used worldwide with impunity.”). When researchers
2 and others discover vulnerabilities, they typically report the flaw to the company
3 responsible for the security of the affected software. If companies are regularly
4 asked to host “watering hole” attacks, they may have conflicting incentives. On the
5 one hand, they might wish to fix such vulnerabilities for the public good; on the
6 other hand, they might be compelled to stockpile such vulnerabilities for future use
7 in a “watering hole” attack.⁷ The stockpiling of zero days can potentially leave
8 millions of individuals as well as companies vulnerable to attack, a perverse
9 situation that has led President Barack Obama’s own Review Group on
10 Intelligence and Communications Technologies to conclude:

11 In almost all instances, for widely used code, it is in the national interest
12 to eliminate software vulnerabilities rather than to use them

13 Eliminating the vulnerabilities — ‘patching’ them — strengthens the
14 security of US Government, critical infrastructure, and other computer
15 systems.

16 Palow Decl. Ex. G at 219-220 [President’s Review Group on Intelligence and
17 Communications Technologies, *Liberty and Security in a Changing World* (Dec.
18 12, 2013)].

19 Now consider the software update process. A software update, also known
20 as a “patch”, is a piece of software released by companies to fix or improve an
21 existing product. Software updates often fix security vulnerabilities, which hackers
22 can otherwise exploit to deliver malware. For this reason, the US government
23 encourages the downloading and installation of software updates as critical cyber

24
25 ⁷ Alternatively, the government, which already stockpiles vulnerabilities, may be incentivized to
26 expand this activity in order to share such vulnerabilities with companies compelled to host
27 “watering hole” attacks. See Palow Decl. Ex. D [*Meet the woman*] (“Hess acknowledged that the
28 bureau uses zero-days—the first time an official has done so. She said the trade-off is one the
bureau wrestles with. ‘What is the greater good—to be able to identify a person who is
threatening public safety?’ Or to alert software makers to bugs that, if unpatched, could leave
consumers vulnerable?”).

1 security measures. For example, a “Mobile Security Tip Card” published by the
2 Department of Homeland Security advises Americans:

3 Install updates for apps and your device’s operating system as soon as
4 they are available. Keeping the software on your mobile device up to date
5 will prevent attackers from being able to take advantage of known
6 vulnerabilities.

7 Palow Decl. Ex. H [Dep’t of Homeland Security, *Mobile Security Tip Card*].

8 Co-opting the software update process is analogous to what the government
9 is asking Apple to do in the Order – that is using the power it claims under the All
10 Writs Act to convert a mechanism traditionally used to improve security into one
11 that subverts it. Should the government seek to do this regularly, which it will if
12 the Court upholds the Order, *see* Palow Decl. Ex. I [Letter to Court, *In re Order*
13 *Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this*
14 *Court*, No. 15-MC-1902 (E.D.N.Y. Feb. 17, 2016), Dkt. 27] (describing twelve
15 other All Writs Act orders against Apple sought by the government); Palow Decl.
16 Ex. J [Martin Kaste, *Slippery Slope? Court Orders Apple to Unlock Shooter’s*
17 *iPhone*, NPR (Feb. 18, 2016)] (quoting Cyrus Vance, Manhattan District Attorney,
18 as stating that he has “about 155 to 160 devices . . . running on iOS 8” that he
19 would like to access), it will fundamentally cripple such core security mechanisms.
20 It will broadly undermine trust in software updates, leading users not to install
21 them. By not installing software updates, consumers will be increasingly
22 vulnerable to security attacks by hackers exploiting unpatched vulnerabilities in the
23 products and services they use.

24 **C. The Order Signals to Other Countries that it is Permissible and**
25 **Appropriate to Compel Technology Companies to Undermine the**
26 **Security of their Products and Services**

27 Many foreign governments are increasingly seeking the power to compel
28 technology companies operating within their jurisdictions to undermine the

1 security of their products both for law enforcement and intelligence-gathering
2 purposes. Emboldened by the US example, these countries may soon place
3 heightened pressure on companies to comply. Technology companies can – and
4 often do – resist these assertions of power in foreign contexts, but it will be
5 increasingly difficult for them to do so should the US government be permitted to
6 assert this power itself.

7 In Russia, for example, the government already claims the power to compel
8 technology companies to assist Russian law enforcement or intelligence agencies
9 in exactly the manner that the US government seeks from Apple, *i.e.* through
10 hacking their own products or services. Article 15 of the Federal Law of the
11 Russian Federation on the Federal Security Service Act (no. 40-FZ) 1995 (“FSB
12 Act”), provides:

13 [L]egal entities in the Russian Federation providing . . . electronic
14 communications services of all types . . . shall be under obligation, at the
15 request of federal security service organs, to include in the apparatus
16 additional hardware and software and create other conditions required . . .
17 to implement operational/technical measures.⁸

18 Palow Decl. Ex. L.⁹ The FSB is a Russian agency that carries out both law
19 enforcement and intelligence activities. *See* Palow Decl. Ex. L, art. 8 [FSB
20 Act] (defining the main activities of the FSB as “counter-intelligence;

21 _____
22 ⁸ In 2012, Eugene Kaspersky, CEO of Kaspersky Lab, which is headquartered in Russia and is
23 one of the world’s largest software security companies, stated that “the FSB ha[d] never made a
24 request to tamper with his software”. Palow Decl. Ex. K [Noah Shachtman, *Russia’s Top Cyber
25 Sleuth Foils US Spies, Helps Kremlin Pals*, *Wired* (July 23, 2012)]. Kaspersky’s statement is
26 important for verifying – at least implicitly – that the FSB possesses the power to make such a
27 request.

28 ⁹ The English translation of this provision is contained in an unofficial translation of the
legislation by the Council of Europe and found at Legislationline.org, which is maintained by the
Organization for Security and Co-operation in Europe. The Library of Congress lists
Legislationline.org as an online resource for finding translations of Russian laws. Palow Decl.
Ex. M at 4 [Law Library of Congress, *Russian Federation Translation of National Legislation
into English* (March 2012)].

1 combating terrorism; combating crime; intelligence; border activity;
2 safeguarding information security”); *see also* Palow Decl. Ex. N, at ¶ 30
3 [Council of Europe, European Commission for Democracy through Law,
4 *Opinion on the Federal Law on the Federal Security Service (FSB) of the*
5 *Russian Federation* (2012)] (describing the FSB as “exercis[ing] considerable
6 powers, including police powers”).

7 The UK is also considering legislation to compel companies to hack their
8 own products or services, and it will only take encouragement from the precedent
9 this Order could set. The Investigatory Powers Bill would authorize UK law
10 enforcement and intelligence agencies to hack electronic devices to obtain
11 “communications” or “any other information”, including through surveillance
12 techniques, such as remotely “listening to a person’s communications or other
13 activities.”¹⁰ Palow Decl. Ex. 0 cl. 88 [Investigatory Powers Bill 2015-16, Bill
14 [143] (Gr. Brit.) [hereinafter “IPB”]]. The Investigatory Powers Bill explicitly
15 compels “telecommunications providers” to assist the UK government in
16 implementing its hacking operations, unless “not reasonably practicable.”¹¹ *Id.* at
17 cl. 111. In addition, the Investigatory Powers Bill authorizes the UK government to
18 issue “National Security Notices” and “Technical Capability Notices”, both of
19 which could compel telecommunications providers to assist the government in
20

21
22 ¹⁰ The Investigatory Powers Bill refers to this power as “equipment interference”, a vague term
23 that may encompass surveillance techniques beyond hacking.

24 ¹¹ The Investigatory Powers Bill defines telecommunications provider as including “a person
25 who . . . offers or provides a telecommunications service to persons in the United Kingdom”.
26 Palow Decl. Ex. O cl. 223(10) [IPB]. In its submission to the Parliamentary committee
27 examining the Investigatory Powers Bill, Apple indicated that “[w]ith the exception of certain
28 limited retail and human resources data, Apple is not established in the UK”, but that the Bill
“makes explicit its reach beyond UK borders to, in effect any service provider with a connection
to UK consumers.” Palow Decl. Ex. P ¶¶ 21-25 [Apple Inc. and Apple Distrib. Int’l, *Written
Evidence to the UK Parliament Joint Comm. on the Draft Investigatory Powers Bill* (IPB0093)
(Jan. 7, 2016) [hereinafter Apple IPB Written Evidence]].

1 vague and sweeping terms.¹² *Id.* at cls. 216-218. All of these powers could be
2 deployed to force technology companies to undermine the security of their own
3 products and services.¹³ Moreover, such powers would be exercised in secret, for
4 the Investigatory Powers Bill gags telecommunications providers from revealing
5 information about any hacking assistance they may have been forced to provide to
6 the government. *Id.* at cls. 114, 218(8).

7 Apple's submission to the Parliamentary committee examining the
8 Investigatory Powers Bill highlights the above concerns. Palow Decl. Ex. P [Apple
9 IPB Written Evidence]. With respect to the hacking provisions in particular, Apple
10 expressed dismay that "the bill could make private companies implicated in the
11 hacking of their customers." *Id.* at ¶ 53. Google, Facebook, Twitter, Yahoo, and
12 Microsoft jointly filed a submission to the committee as well, "reject[ing] any
13 proposals that would require companies to deliberately weaken the security of their
14 products via backdoors, forced decryption, or any other means." Palow Decl. Ex. Q
15 ¶ 3(a) [Facebook Inc., Google Inc., Microsoft Corp., Twitter Inc. and Yahoo Inc.,
16 Written Evidence to the UK Parliamentary Joint Comm. on the Draft Investigatory
17 Powers Bill (IPB0116) (Jan. 7, 2016)]. Apple warned presciently that "[i]f the UK
18

19 ¹² A National Security Notice would require a telecommunications provider "to carry out any
20 conduct, including the provision of services or facilities" where the UK government "considers
21 [it] necessary in the interests of national security." Palow Decl. Ex. O cl. 216 [IPB Bill]. A
22 Technical Capability Notice would require a telecommunications provider to, *inter alia*, "provide
23 facilities or services of a specified description" or "remov[e] . . . electronic protection applied by
24 or on behalf of that operator to any communications or data." *Id.* at cl. 217.

25 ¹³ Compounding concerns about such powers, the Investigatory Powers Bill lacks a meaningful
26 judicial authorization process, as understood in U.S. legal terms, when the U.K. government
27 seeks a warrant to hack. In this scenario, the Home Secretary may issue a warrant subject to
28 "approval" by a Judicial Commissioner ("JC"), which is a new position created by the
Investigatory Powers Bill. *Id.* at cl. 97. Although a JC must have held high judicial office
(defined to include the US equivalent of sitting as a district level judge or above), she is
appointed by the Prime Minister and sits for a term of three years. *Id.* at cls. 194-195. The
Investigatory Powers Bill also places significant limitations on the scrutiny a JC can exercise in
reviewing the warrant. *See id.* at cl. 97. And it does not require any form of judicial approval
with respect to National Security Notices or Technical Capability Notices. *Id.* at cl. 218.

1 Government forces these capabilities, there's no assurance they will not be
2 imposed in other places where protections are absent." Palow Decl. Ex. P ¶ 11
3 [Apple IPB Written Evidence]. That argument applies even more forcefully in the
4 US context. Should the Order stand, Apple and other technology companies will
5 have difficulty mounting credible opposition to the powers the UK government
6 seeks, not least because once the technological capability is developed it will be
7 hard for Apple to refuse to deploy it for other governments.

8 A host of other countries also try to compel technology companies to
9 undermine the security of their products through the use of "backdoors".¹⁴
10 BlackBerry Ltd. ("BlackBerry"), a Canadian company, has wrangled with several
11 countries over whether to grant their agencies backdoor access to its customers'
12 encrypted data. In December 2015, BlackBerry was prepared to shut down
13 operations in Pakistan rather than accede to demands from the government to
14 access encrypted communications sent and received in the country. Palow Decl.
15 Ex. R [Katie Collins, *BlackBerry to leave Pakistan after refusing to ditch user*
16 *privacy*, CNET (Dec. 1, 2015)]. In the past, however, BlackBerry has negotiated
17 arrangements with the United Arab Emirates, Saudi Arabia, and India involving
18 some measure of government access to encrypted data.¹⁵ Palow Decl. Ex. U
19 [Kadhim Shubber, *BlackBerry gives Indian government ability to intercept*
20 *messages*, Wired (July 11, 2013)]; Palow Decl. Ex. V [Lance Whitney, *RIM averts*

21
22 ¹⁴ A backdoor is a method for remotely bypassing security to access a program, computer or
23 network. A backdoor can be a legitimate point of access to allow maintenance by an authorized
24 administrator. It can also be an unauthorized point of access. Apple and others contend that what
25 the government is requesting in this case is a "backdoor." *Amici* submit, as explained above, *see*
26 *supra* p. 6-7, that what the government is asking can also be construed as requiring Apple to
27 hack its own iPhone. Both backdoors and compelled hacking are a serious threat to the security
28 of technology products and services.

¹⁵ BlackBerry has also faced requests for backdoors from Russia and Indonesia; it is unclear how
it resolved those requests. *See* Palow Decl. Ex. S [*Government asks RIM to open access to*
wiretap Blackberry users, Jakarta Post (Sept. 15, 2011)]; Palow Decl. Ex. T [Maria Kiselyova
and Guy Faulconbridge, *BlackBerry firm seeks security 'balance' in Russia*, Reuters (Apr. 25,
2011)].

1 *BlackBerry ban in UAE*, CNET (Oct. 8, 2010)]; Palow Decl. Ex. W [*RIM to share*
2 *some BlackBerry codes with Saudis*, Reuters (Aug. 10, 2010)].

3 Some countries have resorted to “key escrow” systems to try to obtain
4 access to encrypted data.¹⁶ A “key escrow” is a kind of backdoor, in which
5 technology companies offering encryption services (or individuals using
6 encryption) must store copies of decryption keys with the government or a “trusted
7 third party”. Turkey, for example, passed regulations in 2010 “requiring encryption
8 suppliers to provide copies of [decryption] keys to government regulators before
9 offering their encryption tools to users.”¹⁷ Palow Decl. Ex. X ¶ 44 [*2015 Special*
10 *Rapporteur Report*].

11 In 2015, technology companies fought vigorously against a draft
12 Counterterrorism Law in China that would have required both backdoors and a
13 “key escrow” regime. See Palow Decl. Ex. Z [Tom Mitchell, *Obama seeks reboot*
14 *of China cyber laws*, Financial Times (Mar. 3, 2015)] (noting that “US and
15 European corporate executives have expressed alarm over . . . Chinese legislation
16 targeting telecom companies [and] internet service providers”); Palow Decl. Ex.
17 AA [Human Rights Watch, *China: Draft Counterterrorism Law a Recipe for*
18 *Abuses* (Jan. 20, 2015)]. The US government also heavily criticized these
19 measures, with President Barack Obama, Secretary of State John Kerry and US

20 ¹⁶ Some countries simply seek to discourage the use of secure technologies altogether, in
21 manners “tantamount to a ban, such as rules (a) requiring licenses for encryption use; (b) setting
22 weak technical standards for encryption; and (c) controlling the import and export of encryption
23 tools.” Palow Decl. Ex. X ¶ 41 [*Report of the Special Rapporteur on the promotion and*
24 *protection of the right to freedom of opinion and expression, David Kaye, delivered to the*
25 *Human Rights Council*, U.N. Doc. A/HRC/29/32, (May 22, 2015) [hereinafter “*2015 Special*
26 *Rapporteur Report*”]. Countries that regulate in one or more of these manners include Ethiopia,
27 Cuba, and Pakistan. *Id.* at ¶ 41 nn. 28-30.

28 ¹⁷ These regulations are available in English on the website of Turkey’s Information and
Communications Technologies Authority. Palow Decl. Ex. Y art. 5 [Information and
Communication Technologies Authority, By Law on the Procedures and Principles of Encoded
or Encrypted Communication between Public Authorities and Organizations and Real and Legal
Persons in Electronical [sic] Communication Service (Oct. 23, 2010)].

1 Trade Representative Michael Froman advocating against them in direct exchanges
2 with the Chinese government. *See* Palow Decl. Ex. BB [Ankit Panda, *Beijing*
3 *Strikes Back in US-China Tech Wars*, *The Diplomat* (Mar. 6, 2015)]; Palow Decl.
4 Ex. CC [Jeff Mason, *Exclusive: Obama sharply criticizes China's plans for new*
5 *technology rules*, *Reuters* (Mar. 2, 2015)] (“In an interview with Reuters,
6 [President] Obama said he was concerned about Beijing’s plans . . . [to] require
7 technology firms to hand over [decryption] keys, the passcodes that help protect
8 data, and install security ‘backdoors’ in their systems to give Chinese authorities
9 surveillance access.”). The final version of the Counterterrorism Law, which
10 passed in December 2015, softened some of these requirements, a small victory
11 that may not have been won had this Court’s Order existed at the time. *See* Palow
12 Decl. Ex. DD [Samm Sacks, *Apple in China, Part I: What Does Beijing Actually*
13 *Ask of Technology Companies?*, *Lawfare* (Feb. 22, 2016)]. However, the
14 Counterterrorism Law still requires technology companies to provide “technical
15 interfaces, decryption, and other technical assistance and support” and Chinese
16 authorities will be working out the details of the types of assistance companies will
17 be compelled to provide in the coming year.¹⁸ *Id.*

18 China is still in the midst of fleshing out a new legal and regulatory regime
19 governing technology companies. *See id.* It is poised to become Apple’s largest
20 market during this period and Chinese officials will be closely observing the US’s
21 approach to secure technologies. *See* Palow Decl. Ex. EE [Alice Truong, *What*

22 ¹⁸ Decryption usually takes one of two forms: mandatory key disclosure or targeted decryption
23 orders. The former requires disclosure of the key necessary for decryption, permitting the
24 government to access all information protected by the key. The latter requires only that specific
25 information be decrypted and then turned over to the government. Both forms of decryption can
26 require “corporations to cooperate with Governments, creating serious challenges that implicate
27 individual users online.” Palow Decl. Ex. X ¶ 45 [*2015 Special Rapporteur Report*]. Several
28 countries authorize key disclosure by law, including France, Spain and the United Kingdom. *Id.*
at ¶ 45 n.35.

1 *Chinese slowdown? Apple's sales double in China on iPhone growth*, Quartz (Oct.
2 27, 2015)]. In July 2015, the Chinese government released a draft Cybersecurity
3 Law, which outlines obligations for technology companies operating in China. *Id.*
4 Those obligations include requiring that companies “provide unspecified
5 ‘necessary assistance’ to police when investigating crimes and for ‘state security
6 reasons’”. Palow Decl. Ex. FF [Human Rights Watch, *Submission by HRW to the*
7 *National People’s Congress Standing Committee on the draft Cybersecurity Law*
8 (Aug. 4, 2015)]. The outcome of this case and other US government requests to
9 compel companies to undermine the security of their products are likely to
10 influence the final version of the Cybersecurity Law. Indeed, a Chinese official has
11 stated that China studied U.S. and European national laws in drafting the
12 Counterterrorism Law and implied those examples may have influenced its
13 decision to soften its approach. Palow Decl. Ex. GG [*Provisions of China’s*
14 *counterterrorism bill inspired by foreign laws: official*, Xinhua (Dec. 27, 2015)].

15 **D. Other Countries Will Compel Technology Companies to Undermine the**
16 **Security of their Products and Services In Order to Commit Civil and**
17 **Human Rights Abuses**

18 Secure technologies are fundamental to the protection of the right to freedom
19 of expression and opinion. States take advantage of weaknesses in these
20 technologies to attack these rights. These attacks, including through mass
21 surveillance, data collection, and online censorship and filtering, are well
22 documented. *See* Palow Decl. Ex. HH [*Report of the Special Rapporteur on the*
23 *promotion and protection of the right to freedom of opinion and expression, Frank*
24 *La Rue, delivered to the Human Rights Council, U.N. Doc. A/HRC/23/40 (Apr. 23,*
25 *2013)]; Palow Decl. Ex. II ¶ 34 [*Report of the Special Rapporteur on the*
26 *promotion and protection of human rights and fundamental freedoms while*
27 *countering terrorism, Martin Scheinin, delivered to the Human Rights Council,*
28 *U.N. Doc. A/HRC/13/37 (Dec. 28, 2009)] (describing how surveillance measures**

1 in many countries “have a chilling effect on users, who are afraid to visit websites,
2 express their opinions or communicate with other persons for fear that they will
3 face sanctions”). In the face of these attacks, secure technologies:

4 enable private communications and can shield an opinion from outside
5 scrutiny, particularly important in hostile political, social, religious and
6 legal environments. Where States impose unlawful censorship through
7 filtering and other technologies, [they] . . . may empower individuals to
8 circumvent barriers and access information and ideas without the
9 intrusion of authorities. Journalists, researchers, lawyers and civil
10 society rely on [secure technologies] to shield themselves (and their
11 sources, clients and partners) from surveillance and harassment.

12 Palow Decl. Ex. X ¶ 12 [*2015 Special Rapporteur Report*].

13 The US government has also recognized the critical importance of secure
14 technologies to protect the rights to freedom of expression and association. It has
15 voiced its support for “the development and robust adoption of strong encryption,
16 which is a key tool to . . . promote freedoms of expression and association” and is
17 “especially important in sensitive contexts where attribution could have negative
18 political, social or personal consequences or when the privacy interests in the
19 information are strong.” Palow Decl. Ex. JJ, at 1 [U.S. Submission to the Special
20 Rapporteur on the Promotion of the Right to Freedom of Opinion and Expression
21 (Feb. 26, 2015)]. It has accordingly, “as a matter of policy . . . long supported the
22 development and use of strong encryption and anonymity-enabling tools online.”

23 *Id.* at 2. In particular, it has

24 provided funding to support the development and dissemination of anti-
25 censorship and secure communications technologies to ensure that
26 human rights defenders and vulnerable civil society communities, such
27 as journalists, LGBT activists and religious minorities, operating in
28

1 repressive contexts are able [sic] communicate securely, associate
2 safely, and express themselves freely online.

3 *Id.*

4 Secure technologies can also play a vital role in protecting other
5 fundamental civil and human rights. Some states have exploited vulnerabilities in
6 these technologies not only to target activists, dissidents, and political opponents
7 but also to arrest and torture these individuals. *See generally* Palow Decl. Ex. KK
8 [The Right to Privacy in the Digital Age, G.A. Res. 69/166, pmb., U.N. Doc.
9 A/Res/69/166 (Feb. 10, 2014)] (“[n]oting with deep concern that, in many
10 countries, persons and organisations engaged in promoting and defending human
11 rights and fundamental freedoms frequently face threats and harassment and suffer
12 insecurity as well as unlawful or arbitrary interference with their right to privacy as
13 a result of their activities”). The Committee to Protect Journalists, for example, has
14 advised reporters to use encryption tools when communicating with sources in
15 Syria or risk their well-being. Palow Decl. Ex. LL [Eva Galperin, *Don’t get your*
16 *sources in Syria killed*, Committee to Protect Journalists (May 21, 2012)]
17 (describing the Syrian surveillance regime as “extensive” and the use of malware
18 by “pro-Syrian government hackers”). In Bahrain, former political prisoners have
19 reported that they were beaten and interrogated while being shown transcripts of
20 text messages and other communications intercepted by the government. Palow
21 Decl. Ex. MM [Vernon Silver & Ben Elgin, *Torture in Bahrain Becomes Routine*
22 *With Help From Nokia Siemens*, Bloomberg (Aug. 22, 2011)]. Activists and
23 journalists detained in Iran have reported similar incidents. Palow Decl. Ex. NN
24 [Ben Elgin, Vernon Silver & Alan Katz, *Iranian Police Seizing Dissidents Get Aid*
25 *of Western Companies*, Bloomberg (Oct. 31, 2011)] (describing the experience of a
26 journalist who was shown “transcripts of his mobile phone calls, e-mails and text
27 messages during his detention”).
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

V. CONCLUSION

For all of these reasons, Privacy International and HRW strongly urge the Court to consider the wider implications of the Order compelling Apple to assist in the search of the iPhone at issue.

Dated: March 3, 2016

Respectfully submitted,

By 
Caroline Wilson Palow (SBN 241031)
Scarlet Kim
PRIVACY INTERNATIONAL
62 Britton Street
London EC1M 5UY
United Kingdom
Telephone: +44.20.3422.4321
caroline@privacyinternational.org


Attorneys for *Amici Curiae*
Privacy International and
Human Rights Watch

	1900 M Street N.W., Suite 250 Washington, D.C. 20036 Telephone: (202) 706-5202 Facsimile: (202) 706-5298 Email: marc@zwillgen.com jeff@zwillgen.com	
Mail & E-mail	Eileen M. Decker Patricia A. Donahue Tracy L. Wilkison Allen W. Chui 1500 United States Courthouse 7312 North Spring Street Los Angeles, California 90012 Telephone: (213) 894-0622/2435 Facsimile: (213) 894-8601-7520 Email: Tracy.Wilkison@usdoj.gov Allen.Chiu@usdoj.gov	United States of America

*Apple, Inc. has consented in writing to service by electronic means in accordance with Federal Rule of Civil Procedure 5(b)(E), Local Civil Rule 5-3.1.1, and Local Criminal Rule 49-1.3.2(b).

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct and that I have made service at the direction of a member of the bar of this Court.

Executed on March 3, 2016 in London, United Kingdom

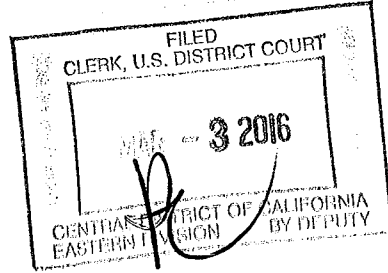


 Sara Nelson

ORIGINAL

SCANNED

1 CAROLINE WILSON PALOW (SBN 241031)
 2 caroline@privacyinternational.org
 3 SCARLET KIM
 4 scarlet@privacyinternational.org
 5 PRIVACY INTERNATIONAL
 6 62 Britton Street
 7 London EC1M 5UY
 8 United Kingdom
 9 Telephone: +44.20.3422.4321



8 Attorneys for *Amici Curiae*
 9 PRIVACY INTERNATIONAL
 10 HUMAN RIGHTS WATCH

LODGED

2016 MAR -3 PM 1:50
 CLERK U.S. DISTRICT COURT
 CENTRAL DIST. OF CALIF.
 RIVERSIDE

11 UNITED STATES DISTRICT COURT
 12 CENTRAL DISTRICT OF CALIFORNIA
 13 EASTERN DIVISION

14
 15 IN THE MATTER OF THE SEARCH) ED No. CM 16-10 (SP)
 16 OF AN APPLE IPHONE SEIZED)
 17 DURING THE EXECUTION OF A) **DECLARATION OF CAROLINE**
 18 SEARCH WARRANT ON A BLACK) **WILSON PALOW IN SUPPORT OF**
 19 LEXUS IS300, CALIFORNIA) **BRIEF OF AMICI CURIAE**
 20 LICENSE PLATE 35KGD203) **PRIVACY INTERNATIONAL AND**
 21) **HUMAN RIGHTS WATCH**
 22)
 23) **Hearing:**
 24) Date: March 22, 2016
 25) Time: 1:00 p.m.
 26) Place: Courtroom 3 or 4
 27) Judge: Hon. Sheri Pym
 28

1 tools/2015/12/08/15adb35e-9860-11e5-8917-653b65c809eb_story.html. The
2 article was printed on March 2, 2016.

3 6. Attached hereto as **Exhibit E** is a true and correct copy of the
4 Washington Post article, *Forbes Web site was compromised by Chinese*
5 *cyberespionage group, researchers say*, by Andrea Peterson, originally published
6 on February 10, 2015, available at [https://www.washingtonpost.com/news/the-](https://www.washingtonpost.com/news/the-switch/wp/2015/02/10/forbes-web-site-was-compromised-by-chinese-cyberespionage-group-researchers-say/)
7 [switch/wp/2015/02/10/forbes-web-site-was-compromised-by-chinese-](https://www.washingtonpost.com/news/the-switch/wp/2015/02/10/forbes-web-site-was-compromised-by-chinese-cyberespionage-group-researchers-say/)
8 [cyberespionage-group-researchers-say/](https://www.washingtonpost.com/news/the-switch/wp/2015/02/10/forbes-web-site-was-compromised-by-chinese-cyberespionage-group-researchers-say/). The article was printed on March 2,
9 2016.

10 7. Attached hereto as **Exhibit F** is a true and correct copy of an excerpt
11 from the book *Data and Goliath*, by Bruce Schneier, originally published in 2015.
12 The excerpt was copied on March 2, 2016.

13 8. Attached hereto as **Exhibit G** is a true and correct copy of an excerpt
14 from the report of the President's Review Group on Intelligence and
15 Communications Technologies, entitled *Liberty and Security in a Changing*
16 *World*, originally published on December 12, 2013, available at
17 [https://www.whitehouse.gov/sites/default/files/docs/2013-12-](https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf)
18 [12_rg_final_report.pdf](https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf). The excerpt was printed on March 2, 2016.

19 9. Attached hereto as **Exhibit H** is a true and correct copy of the US
20 Department of Homeland Security's "Mobile Security Tip Card," originally
21 published as part of the Stop.Think.Connect. campaign, available at
22 [https://www.dhs.gov/sites/default/files/publications/Mobile%20Security%20Tip](https://www.dhs.gov/sites/default/files/publications/Mobile%20Security%20Tip%20Card_3.pdf)
23 [%20Card_3.pdf](https://www.dhs.gov/sites/default/files/publications/Mobile%20Security%20Tip%20Card_3.pdf). The tip card was printed on March 2, 2016.

24 10. Attached hereto as **Exhibit I** is a true and correct copy of the Letter to
25 the Court filed by Apple Inc. on February 17, 2016 in *In re Order Requiring*
26 *Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*,
27 No. 15-MC-1902 (E.D.N.Y.), Dkt. 27.
28

1 11. Attached hereto as **Exhibit J** is a true and correct copy of the NPR
2 article, *Slippery Slope? Court Orders Apple to Unlock Shooter's iPhone*, by
3 Martin Kaste, originally published on February 18, 2016, available at
4 [http://www.npr.org/2016/02/18/467176553/slippy-slope-court-orders-apple-to-](http://www.npr.org/2016/02/18/467176553/slippy-slope-court-orders-apple-to-unlock-shooter-s-iphone)
5 [unlock-shooter-s-iphone](http://www.npr.org/2016/02/18/467176553/slippy-slope-court-orders-apple-to-unlock-shooter-s-iphone). The article was printed on March 2, 2016.

6 12. Attached hereto as **Exhibit K** is a true and correct copy of an English
7 translation of article 15 of the Federal Law of the Russian Federation on the
8 Federal Security Service Act (no. 40-FZ) 1995, created by the Council of Europe,
9 available at
10 http://www.legislationline.org/download/action/download/id/3708/file/RF_law_fe
11 [d_security_service_1999_am2011_en.pdf](http://www.legislationline.org/download/action/download/id/3708/file/RF_law_fe). Legislationline.org is a site maintained
12 by the Organization for Security and Co-operation in Europe. The translation was
13 printed on March 2, 2016.

14 13. Attached hereto as **Exhibit L** is a true and correct copy of the Library
15 of Congress's guide to translations of Russian legislation into English, *Russian*
16 *Federation: Translation of National Legislation into English*, originally published
17 in 2012, available at [https://www.loc.gov/law/find/pdfs/2012-](https://www.loc.gov/law/find/pdfs/2012-007612_RU_RPT.pdf)
18 [007612_RU_RPT.pdf](https://www.loc.gov/law/find/pdfs/2012-007612_RU_RPT.pdf). The guide lists legislationline.org as an online resource for
19 finding such translations. The guide was printed on March 2, 2016.

20 14. Attached hereto as **Exhibit M** is a true and correct copy of the Wired
21 article, *Russia's Top Cyber Sleuth Foils US Spies, Helps Kremlin Pals*, by Noah
22 Shachtman, originally published on July 23, 2012, available at
23 http://www.wired.com/2012/07/ff_kaspersky/. The article was printed on March
24 2, 2016.

25 15. Attached hereto as **Exhibit N** is a true and correct copy of the report,
26 *Opinion on the Federal Law on the Federal Security Service (FSB) of the Russian*
27 *Federation*, by the Council of Europe's European Commission for Democracy
28 through Law, originally published on June 20, 2012, available at

1 <http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL->
2 [AD\(2012\)015-e](http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2012)015-e). The article was printed on March 2, 2016.

3 16. Attached hereto as **Exhibit O** is a true and correct copy of excerpts of
4 the Investigatory Powers Bill, Bill 143, introduced to the UK Parliament on
5 March 1, 2016, available at
6 <http://www.publications.parliament.uk/pa/bills/cbill/2015-2016/0143/16143.pdf>.
7 The excerpts were printed on March 2, 2016.

8 17. Attached hereto as **Exhibit P** is a true and correct copy of the written
9 evidence (IPB0093) presented by Apple Inc. and Apple Distribution International
10 to the UK Joint Committee on the Draft Investigatory Powers Bill, originally
11 published on January 7, 2016, available at
12 <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocum>
13 [ent/draft-investigatory-powers-bill-committee/draft-investigatory-powers-](http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/26341.html)
14 [bill/written/26341.html](http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/26341.html). The evidence was printed on March 2, 2016.

15 18. Attached hereto as **Exhibit Q** is a true and correct copy of the written
16 evidence (IPB0116) presented by Facebook Inc., Google Inc., Microsoft Corp.,
17 Twitter Inc. and Yahoo Inc. to the UK Joint Committee on the Draft Investigatory
18 Powers Bill, originally published on January 7, 2016, available at
19 <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocum>
20 [ent/draft-investigatory-powers-bill-committee/draft-investigatory-powers-](http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/26367.html)
21 [bill/written/26367.html](http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/26367.html). The evidence was printed on March 2, 2016.

22 19. Attached hereto as **Exhibit R** is a true and correct copy of the CNET
23 article, *BlackBerry to leave Pakistan after refusing to ditch user privacy*, by Katie
24 Collins, originally published on December 1, 2015, available at
25 [http://www.cnet.com/au/news/blackberry-leaves-pakistan-after-refusing-to-](http://www.cnet.com/au/news/blackberry-leaves-pakistan-after-refusing-to-compromise-user-privacy/)
26 [compromise-user-privacy/](http://www.cnet.com/au/news/blackberry-leaves-pakistan-after-refusing-to-compromise-user-privacy/). The article was printed on March 2, 2016.

27 20. Attached hereto as **Exhibit S** is a true and correct copy of the Jakarta
28 Post article, *Government asks RIM to open access to wiretap Blackberry users*,

1 *Jakarta Post*, originally published on September 15, 2011, available at
2 <http://www.thejakartapost.com/news/2011/09/15/government-asks-rim-open->
3 [access-wiretap-blackberry-users.html](http://www.thejakartapost.com/news/2011/09/15/government-asks-rim-open-access-wiretap-blackberry-users.html). The article was printed on March 2, 2016.

4 21. Attached hereto as **Exhibit T** is a true and correct copy of the Reuters
5 article, *BlackBerry firm seeks security 'balance' in Russia*, by Maria Kiselyova &
6 Guy Faulconbridge, originally published on April 25, 2011, available at
7 <http://www.reuters.com/article/us-blackberry-russia-idUSTRE73O1ZL20110425>.
8 The article was printed on March 2, 2016.

9 22. Attached hereto as **Exhibit U** is a true and correct copy of the Wired
10 article, *BlackBerry gives Indian government ability to intercept message*, by
11 Kadhim Shubber, originally published on July 11, 2013, available at
12 <http://www.wired.co.uk/news/archive/2013-07/11/blackberry-india>. The article
13 was printed on March 2, 2016.

14 23. Attached hereto as **Exhibit V** is a true and correct copy of the CNET
15 article, *RIM averts BlackBerry ban in UAE*, by Lance Whitney, originally
16 published on October 8, 2010, available at [http://www.cnet.com/news/rim-averts-](http://www.cnet.com/news/rim-averts-blackberry-ban-in-uae/)
17 [blackberry-ban-in-uae/](http://www.cnet.com/news/rim-averts-blackberry-ban-in-uae/). The article was printed on March 2, 2016.

18 24. Attached hereto as **Exhibit W** is a true and correct copy of the
19 Reuters article, *RIM to share some BlackBerry codes with Saudis*, originally
20 published on August 10, 2010, available at [http://www.reuters.com/article/us-](http://www.reuters.com/article/us-blackberry-saudi-idUSTRE6751Q220100810)
21 [blackberry-saudi-idUSTRE6751Q220100810](http://www.reuters.com/article/us-blackberry-saudi-idUSTRE6751Q220100810). The article was printed on March
22 2, 2016.

23 25. Attached hereto as **Exhibit X** is a true and correct copy of the *Report*
24 *of the Special Rapporteur on the promotion and protection of the right to freedom*
25 *of opinion and expression, David Kaye* (U.N. Doc. A/HRC/29/32), delivered to
26 the Human Rights Council on May 22, 2015, available at
27 [http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Document](http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc)
28 [s/A.HRC.29.32_AEV.doc](http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc). The report was printed on March 2, 2016.

1 26. Attached hereto as **Exhibit Y** is a true and correct copy of an English
2 translation of the By Law on the Procedures and Principles of Encoded or
3 Encrypted Communication between Public Authorities and Organizations and
4 Real and Legal Persons in Electronical [sic] Communication Service, dated
5 October 23, 2010, by Turkey's Information and Communication Technologies
6 Authority, which can be found on [http://www.btk.gov.tr/en-](http://www.btk.gov.tr/en-US/Ordinances?page=3)
7 [US/Ordinances?page=3](http://www.btk.gov.tr/en-US/Ordinances?page=3). The translation was printed on March 2, 2016.

8 27. Attached hereto as **Exhibit Z** is a true and correct copy of the
9 Financial Times article, *Obama seeks reboot of China cyber laws*, by Tom
10 Mitchell, originally published on March 3, 2015, available at
11 [http://www.ft.com/cms/s/0/feb4dc18-c16e-11e4-8b74-](http://www.ft.com/cms/s/0/feb4dc18-c16e-11e4-8b74-00144feab7de.html#axzz41lbGasJD)
12 [00144feab7de.html#axzz41lbGasJD](http://www.ft.com/cms/s/0/feb4dc18-c16e-11e4-8b74-00144feab7de.html#axzz41lbGasJD). The article was printed on March 2, 2016.

13 28. Attached hereto as **Exhibit AA** is a true and correct copy of a Human
14 Rights Watch blog post, *China: Draft Counterterrorism Law a Recipe for Abuses*,
15 originally published on January 20, 2015, available at
16 [https://www.hrw.org/news/2015/01/20/china-draft-counterterrorism-law-recipe-](https://www.hrw.org/news/2015/01/20/china-draft-counterterrorism-law-recipe-abuses)
17 [abuses](https://www.hrw.org/news/2015/01/20/china-draft-counterterrorism-law-recipe-abuses). The post was printed on March 2, 2016.

18 29. Attached hereto as **Exhibit BB** is a true and correct copy of The
19 Diplomat article, *Beijing Strikes Back in US-China Tech Wars*, by Ankit Panda,
20 originally published on March 6, 2015, available at
21 <http://thediplomat.com/2015/03/beijing-strikes-back-in-us-china-tech-wars/>. The
22 article was printed on March 2, 2016.

23 30. Attached hereto as **Exhibit CC** is a true and correct copy of the
24 Reuters article, *Exclusive: Obama sharply criticizes China's plans for new*
25 *technology rules*, by Jeff Mason, originally published on March 2, 2015, available
26 at [http://www.reuters.com/article/us-usa-obama-china-](http://www.reuters.com/article/us-usa-obama-china-idUSKBN0LY2H520150302)
27 [idUSKBN0LY2H520150302](http://www.reuters.com/article/us-usa-obama-china-idUSKBN0LY2H520150302). The article was printed on March 2, 2016.

1 31. Attached hereto as **Exhibit DD** is a true and correct copy of the
2 Lawfare blog post, *Apple in China, Part I: What Does Beijing Actually Ask of*
3 *Technology Companies?*, by Samm Sacks, originally published on February 22,
4 2016, available at [https://www.lawfareblog.com/apple-china-part-i-what-does-](https://www.lawfareblog.com/apple-china-part-i-what-does-beijing-actually-ask-technology-companies)
5 [beijing-actually-ask-technology-companies](https://www.lawfareblog.com/apple-china-part-i-what-does-beijing-actually-ask-technology-companies). The post was published on March 2,
6 2016.

7 32. Attached hereto as **Exhibit EE** is a true and correct copy of the
8 Quartz article, *What Chinese slowdown? Apple's sales double in China on iPhone*
9 *growth*, by Alice Truong, originally published on October 27, 2015, available at
10 [http://qz.com/534907/what-chinese-slowdown-apples-sales-double-in-china-on-](http://qz.com/534907/what-chinese-slowdown-apples-sales-double-in-china-on-iphone-growth/)
11 [iphone-growth/](http://qz.com/534907/what-chinese-slowdown-apples-sales-double-in-china-on-iphone-growth/). The article was published on March 2, 2016.

12 33. Attached hereto as **Exhibit FF** is a true and correct copy of the
13 submission by Human Rights Watch to China's National People's Congress
14 Standing Committee on the draft Cybersecurity Law, originally published on
15 August 4, 2015, available at [https://www.hrw.org/news/2015/08/04/hrw-](https://www.hrw.org/news/2015/08/04/hrw-submission-draft-cybersecurity-law)
16 [submission-draft-cybersecurity-law](https://www.hrw.org/news/2015/08/04/hrw-submission-draft-cybersecurity-law). The letter was published on March 2, 2016.

17 34. Attached hereto as **Exhibit GG** is a true and correct copy of the
18 Xinhua article, *Provisions of China's counterterrorism bill inspired by foreign*
19 *laws: official*, originally published on December 27, 2015, available at
20 http://news.xinhuanet.com/english/2015-12/27/c_134955785.htm. The letter was
21 published on March 2, 2016.

22 35. Attached hereto as **Exhibit HH** is a true and correct copy of the
23 *Report of the Special Rapporteur on the promotion and protection of the right to*
24 *freedom of opinion and expression, Frank La Rue* (U.N. Doc. A/HRC/23/40),
25 delivered to the Human Rights Council on April 23, 2013, available at
26 [http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session](http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf)
27 [23/A.HRC.23.40_EN.pdf](http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf). The report was printed on March 2, 2016.

1 36. Attached hereto as **Exhibit II** is a true and correct copy of the *Report*
2 *of the Special Rapporteur on the promotion and protection of human rights and*
3 *fundamental freedoms while countering terrorism, Martin Sheinin* (U.N. Doc.
4 A/HRC/13/37), delivered to the Human Rights Council on December 28, 2009,
5 available at [http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-](http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf)
6 [HRC-13-37.pdf](http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf). The report was printed on March 2, 2016.

7 37. Attached hereto as **Exhibit JJ** is a true and correct copy of the
8 submission by the United States to the Special Rapporteur on the Promotion of
9 the Right to Freedom of Opinion and Expression, originally published on
10 February 27, 2015, available at
11 [http://www.ohchr.org/Documents/Issues/Opinion/Communications/States/USA.p](http://www.ohchr.org/Documents/Issues/Opinion/Communications/States/USA.pdf)
12 [df](http://www.ohchr.org/Documents/Issues/Opinion/Communications/States/USA.pdf). The report was printed on March 2, 2016.

13 38. Attached hereto as **Exhibit KK** is a true and correct copy of the
14 Resolution adopted by the UN General Assembly on December 18, 2014 at the
15 69th session of the UN (U.N. Doc. A/RES/69/166), *The right to privacy in the*
16 *digital age*, available at
17 http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/69/166. The
18 resolution was printed on March 2, 2016.

19 39. Attached hereto as **Exhibit LL** is a true and correct copy of the
20 Committee to Protect Journalists' blog post, *Don't get your sources in Syria*
21 *killed*, by Eva Galperin, originally published on May 21, 2012, available at
22 <https://cpj.org/blog/2012/05/dont-get-your-sources-in-syria-killed.php>. The post
23 was printed on March 2, 2016.

24 40. Attached hereto as **Exhibit MM** is a true and correct copy of the
25 Bloomberg article, *Torture in Bahrain Becomes Routine With Help From Nokia*
26 *Siemens*, by Vernon Silver and Ben Elgin, originally published on August 22,
27 2011, available at <http://www.bloomberg.com/news/articles/2011-08-22/torture->
28

1 in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking. The post
2 was printed on March 2, 2016.

3 41. Attached hereto as **Exhibit NN** is a true and correct copy of the
4 Bloomberg article, *Iranian Police Seizing Dissidents Get Aid of Western*
5 *Companies*, by Ben Elgin, Vernon Silver and Alan Katz, originally published on
6 October 31, 2011, available at [http://www.bloomberg.com/news/articles/2011-10-](http://www.bloomberg.com/news/articles/2011-10-31/iranian-police-seizing-dissidents-get-aid-of-western-companies)
7 [31/iranian-police-seizing-dissidents-get-aid-of-western-companies](http://www.bloomberg.com/news/articles/2011-10-31/iranian-police-seizing-dissidents-get-aid-of-western-companies). The post was
8 printed on March 2, 2016.

9 I declare under penalty of perjury of the laws of the United States that the
10 foregoing is true and correct. Executed in London, United Kingdom on March 3,
11 2016.


12
13
14
15 
16 Caroline Wilson Palow
17
18
19
20
21
22
23
24
25
26
27
28

Exhibit A



iOS Security

iOS 9.0 or later

September 2015

Contents

Page 4	Introduction
Page 5	System Security Secure boot chain System Software Authorization Secure Enclave Touch ID
Page 10	Encryption and Data Protection Hardware security features File Data Protection Passcodes Data Protection classes Keychain Data Protection Access to Safari saved passwords Keybags Security Certifications and programs
Page 18	App Security App code signing Runtime process security Extensions App Groups Data Protection in apps Accessories HomeKit HealthKit Apple Watch
Page 27	Network Security TLS VPN Wi-Fi Bluetooth Single Sign-on AirDrop security
Page 31	Apple Pay Apple Pay components How Apple Pay uses the Secure Element How Apple Pay uses the NFC controller Credit and debit card provisioning Payment authorization Transaction-specific dynamic security code Contactless payments with Apple Pay Paying with Apple Pay within apps Rewards cards Suspending, removing, and erasing cards

Page 38 Internet Services

- Apple ID
- iMessage
- FaceTime
- iCloud
- iCloud Keychain
- Siri
- Continuity
- Spotlight Suggestions

Page 50 Device Controls

- Passcode protection
- iOS pairing model
- Configuration enforcement
- Mobile device management (MDM)
- Device Enrollment Program
- Apple Configurator
- Device restrictions
- Supervised-only restrictions
- Remote wipe
- Find My iPhone and Activation Lock

Page 56 Privacy Controls

- Location Services
- Access to personal data
- Privacy policy

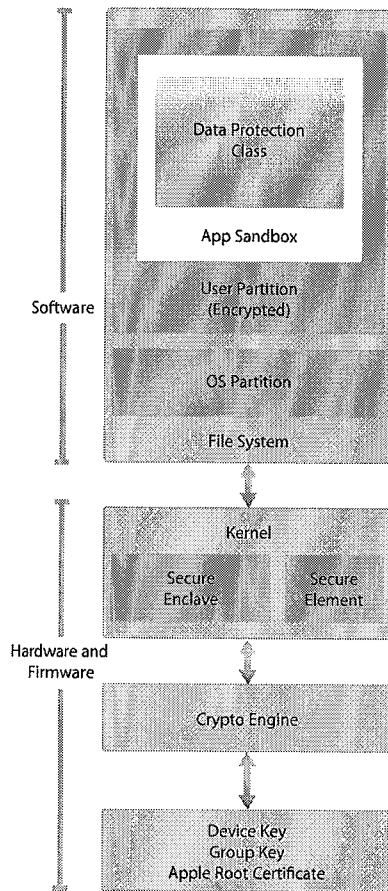
Page 57 Conclusion

- A commitment to security

Page 58 Glossary

Page 60 Document Revision History

Introduction



Security architecture diagram of iOS provides a visual overview of the different technologies discussed in this document.

Apple designed the iOS platform with security at its core. When we set out to create the best possible mobile platform, we drew from decades of experience to build an entirely new architecture. We thought about the security hazards of the desktop environment, and established a new approach to security in the design of iOS. We developed and incorporated innovative features that tighten mobile security and protect the entire system by default. As a result, iOS is a major leap forward in security for mobile devices.

Every iOS device combines software, hardware, and services designed to work together for maximum security and a transparent user experience. iOS protects not only the device and its data at rest, but the entire ecosystem, including everything users do locally, on networks, and with key Internet services.

iOS and iOS devices provide advanced security features, and yet they're also easy to use. Many of these features are enabled by default, so IT departments don't need to perform extensive configurations. And key security features like device encryption are not configurable, so users can't disable them by mistake. Other features, such as Touch ID, enhance the user experience by making it simpler and more intuitive to secure the device.

This document provides details about how security technology and features are implemented within the iOS platform. It will also help organizations combine iOS platform security technology and features with their own policies and procedures to meet their specific security needs.

This document is organized into the following topic areas:

- **System security:** The integrated and secure software and hardware that are the platform for iPhone, iPad, and iPod touch.
- **Encryption and data protection:** The architecture and design that protects user data if the device is lost or stolen, or if an unauthorized person attempts to use or modify it.
- **App security:** The systems that enable apps to run securely and without compromising platform integrity.
- **Network security:** Industry-standard networking protocols that provide secure authentication and encryption of data in transmission.
- **Apple Pay:** Apple's implementation of secure payments.
- **Internet services:** Apple's network-based infrastructure for messaging, syncing, and backup.
- **Device controls:** Methods that prevent unauthorized use of the device and enable it to be remotely wiped if lost or stolen.
- **Privacy controls:** Capabilities of iOS that can be used to control access to Location Services and user data.

System Security

Entering Device Firmware Upgrade (DFU) mode

Restoring a device after it enters DFU mode returns it to a known good state with the certainty that only unmodified Apple-signed code is present. DFU mode can be entered manually: First connect the device to a computer using a USB cable, then hold down both the Home and Sleep/Wake buttons. After 8 seconds, release the Sleep/Wake button while continuing to hold down the Home button. Note: Nothing will be displayed on the screen when the device is in DFU mode. If the Apple logo appears, the Sleep/Wake button was held down too long.

System security is designed so that both software and hardware are secure across all core components of every iOS device. This includes the boot-up process, software updates, and Secure Enclave. This architecture is central to security in iOS, and never gets in the way of device usability.

The tight integration of hardware and software on iOS devices ensures that each component of the system is trusted, and validates the system as a whole. From initial boot-up to iOS software updates to third-party apps, each step is analyzed and vetted to help ensure that the hardware and software are performing optimally together and using resources properly.

Secure boot chain

Each step of the startup process contains components that are cryptographically signed by Apple to ensure integrity and that proceed only after verifying the chain of trust. This includes the bootloaders, kernel, kernel extensions, and baseband firmware.

When an iOS device is turned on, its application processor immediately executes code from read-only memory known as the Boot ROM. This immutable code, known as the hardware root of trust, is laid down during chip fabrication, and is implicitly trusted. The Boot ROM code contains the Apple Root CA public key, which is used to verify that the Low-Level Bootloader (LLB) is signed by Apple before allowing it to load. This is the first step in the chain of trust where each step ensures that the next is signed by Apple. When the LLB finishes its tasks, it verifies and runs the next-stage bootloader, iBoot, which in turn verifies and runs the iOS kernel.

This secure boot chain helps ensure that the lowest levels of software are not tampered with and allows iOS to run only on validated Apple devices.

For devices with cellular access, the baseband subsystem also utilizes its own similar process of secure booting with signed software and keys verified by the baseband processor.

For devices with an A7 or later A-series processor, the Secure Enclave coprocessor also utilizes a secure boot process that ensures its separate software is verified and signed by Apple.

If one step of this boot process is unable to load or verify the next process, startup is stopped and the device displays the "Connect to iTunes" screen. This is called recovery mode. If the Boot ROM is not able to load or verify LLB, it enters DFU (Device Firmware Upgrade) mode. In both cases, the device must be connected to iTunes via USB and restored to factory default settings. For more information on manually entering recovery mode, see <https://support.apple.com/kb/HT1808>.

System Software Authorization

Apple regularly releases software updates to address emerging security concerns and also provide new features; these updates are provided for all supported devices simultaneously. Users receive iOS update notifications on the device and through iTunes, and updates are delivered wirelessly, encouraging rapid adoption of the latest security fixes.

The startup process described above helps ensure that only Apple-signed code can be installed on a device. To prevent devices from being downgraded to older versions that lack the latest security updates, iOS uses a process called *System Software Authorization*. If downgrades were possible, an attacker who gains possession of a device could install an older version of iOS and exploit a vulnerability that's been fixed in the newer version.

On a device with an A7 or later A-series processor, the Secure Enclave coprocessor also utilizes System Software Authorization to ensure the integrity of its software and prevent downgrade installations. See "Secure Enclave," below.

iOS software updates can be installed using iTunes or over the air (OTA) on the device. With iTunes, a full copy of iOS is downloaded and installed. OTA software updates download only the components required to complete an update, improving network efficiency, rather than downloading the entire OS. Additionally, software updates can be cached on a local network server running the caching service on OS X Server so that iOS devices do not need to access Apple servers to obtain the necessary update data.

During an iOS upgrade, iTunes (or the device itself, in the case of OTA software updates) connects to the Apple installation authorization server and sends it a list of cryptographic measurements for each part of the installation bundle to be installed (for example, LLB, iBoot, the kernel, and OS image), a random anti-replay value (nonce), and the device's unique ID (ECID).

The authorization server checks the presented list of measurements against versions for which installation is permitted and, if it finds a match, adds the ECID to the measurement and signs the result. The server passes a complete set of signed data to the device as part of the upgrade process. Adding the ECID "personalizes" the authorization for the requesting device. By authorizing and signing only for known measurements, the server ensures that the update takes place exactly as provided by Apple.

The boot-time chain-of-trust evaluation verifies that the signature comes from Apple and that the measurement of the item loaded from disk, combined with the device's ECID, matches what was covered by the signature.

These steps ensure that the authorization is for a specific device and that an old iOS version from one device can't be copied to another. The nonce prevents an attacker from saving the server's response and using it to tamper with a device or otherwise alter the system software.

Secure Enclave

The Secure Enclave is a coprocessor fabricated in the Apple A7 or later A-series processor. It utilizes its own secure boot and personalized software update separate from the application processor. It provides all cryptographic operations for Data Protection key management and maintains the integrity of Data Protection even if the kernel has been compromised.

The Secure Enclave uses encrypted memory and includes a hardware random number generator. Its microkernel is based on the L4 family, with modifications by Apple. Communication between the Secure Enclave and the application processor is isolated to an interrupt-driven mailbox and shared memory data buffers.

Each Secure Enclave is provisioned during fabrication with its own UID (Unique ID) that is not accessible to other parts of the system and is not known to Apple. When the device starts up, an ephemeral key is created, entangled with its UID, and used to encrypt the Secure Enclave's portion of the device's memory space.

Additionally, data that is saved to the file system by the Secure Enclave is encrypted with a key entangled with the UID and an anti-replay counter.

The Secure Enclave is responsible for processing fingerprint data from the Touch ID sensor, determining if there is a match against registered fingerprints, and then enabling access or purchases on behalf of the user. Communication between the processor and the Touch ID sensor takes place over a serial peripheral interface bus. The processor forwards the data to the Secure Enclave but cannot read it. It's encrypted and authenticated with a session key that is negotiated using the device's shared key that is provisioned for the Touch ID sensor and the Secure Enclave. The session key exchange uses AES key wrapping with both sides providing a random key that establishes the session key and uses AES-CCM transport encryption.

Touch ID

Touch ID is the fingerprint sensing system that makes secure access to the device faster and easier. This technology reads fingerprint data from any angle and learns more about a user's fingerprint over time, with the sensor continuing to expand the fingerprint map as additional overlapping nodes are identified with each use.

Touch ID makes using a longer, more complex passcode far more practical because users won't have to enter it as frequently. Touch ID also overcomes the inconvenience of a passcode-based lock, not by replacing it but by securely providing access to the device within thoughtful boundaries and time constraints.

Touch ID and passcodes

To use Touch ID, users must set up their device so that a passcode is required to unlock it. When Touch ID scans and recognizes an enrolled fingerprint, the device unlocks without asking for the device passcode. The passcode can always be used instead of Touch ID, and it's still required under the following circumstances:

- The device has just been turned on or restarted.
- The device has not been unlocked for more than 48 hours.
- The device has received a remote lock command.
- After five unsuccessful attempts to match a fingerprint.
- When setting up or enrolling new fingers with Touch ID.

When Touch ID is enabled, the device immediately locks when the Sleep/Wake button is pressed. With passcode-only security, many users set an unlocking grace period to avoid having to enter a passcode each time the device is used. With Touch ID, the device locks every time it goes to sleep, and requires a fingerprint—or optionally the passcode—at every wake.

Touch ID can be trained to recognize up to five different fingers. With one finger enrolled, the chance of a random match with someone else is 1 in 50,000. However, Touch ID allows only five unsuccessful fingerprint match attempts before the user is required to enter a passcode to obtain access.

Other uses for Touch ID

Touch ID can also be configured to approve purchases from the iTunes Store, the App Store, and the iBooks Store, so users don't have to enter an Apple ID password. When they choose to authorize a purchase, authentication tokens are exchanged between the device and the store. The token and cryptographic nonce are held in the Secure Enclave. The nonce is signed with a Secure Enclave key shared by all devices and the iTunes Store.

Touch ID can also be used with Apple Pay, Apple's implementation of secure payments. For more information, see the Apple Pay section of this document.

Additionally, third-party apps can use system-provided APIs to ask the user to authenticate using Touch ID or a passcode. The app is only notified as to whether the authentication was successful; it cannot access Touch ID or the data associated with the enrolled fingerprint.

Keychain items can also be protected with Touch ID, to be released by the Secured Enclave only by a fingerprint match or the device passcode. App developers also have APIs to verify that a passcode has been set by the user and therefore able to authenticate or unlock keychain items using Touch ID.

With iOS 9, developers can require that Touch ID API operations don't fall back to an application password or the device passcode. Along with the ability to retrieve a representation of the state of enrolled fingers, this allows Touch ID to be used as a second factor in security sensitive apps.

Touch ID security

The fingerprint sensor is active only when the capacitive steel ring that surrounds the Home button detects the touch of a finger, which triggers the advanced imaging array to scan the finger and send the scan to the Secure Enclave.

The raster scan is temporarily stored in encrypted memory within the Secure Enclave while being vectorized for analysis, and then it's discarded. The analysis utilizes subdermal ridge flow angle mapping, which is a lossy process that discards minutia data that would be required to reconstruct the user's actual fingerprint. The resulting map of nodes is stored without any identity information in an encrypted format that can only be read by the Secure Enclave, and is never sent to Apple or backed up to iCloud or iTunes.

How Touch ID unlocks an iOS device

If Touch ID is turned off, when a device locks, the keys for Data Protection class Complete, which are held in the Secure Enclave, are discarded. The files and keychain items in that class are inaccessible until the user unlocks the device by entering his or her passcode.

With Touch ID turned on, the keys are not discarded when the device locks; instead, they're wrapped with a key that is given to the Touch ID subsystem inside the Secure Enclave. When a user attempts to unlock the device, if Touch ID recognizes the user's fingerprint, it provides the key for unwrapping the Data Protection keys, and the device is unlocked. This process provides additional protection by requiring the Data Protection and Touch ID subsystems to cooperate in order to unlock the device.

The keys needed for Touch ID to unlock the device are lost if the device reboots and are discarded by the Secure Enclave after 48 hours or five failed Touch ID recognition attempts.

Encryption and Data Protection

The secure boot chain, code signing, and runtime process security all help to ensure that only trusted code and apps can run on a device. iOS has additional encryption and data protection features to safeguard user data, even in cases where other parts of the security infrastructure have been compromised (for example, on a device with unauthorized modifications). This provides important benefits for both users and IT administrators, protecting personal and corporate information at all times and providing methods for instant and complete remote wipe in the case of device theft or loss.

Hardware security features

On mobile devices, speed and power efficiency are critical. Cryptographic operations are complex and can introduce performance or battery life problems if not designed and implemented with these priorities in mind.

Every iOS device has a dedicated AES 256 crypto engine built into the DMA path between the flash storage and main system memory, making file encryption highly efficient.

The device's unique ID (UID) and a device group ID (GID) are AES 256-bit keys fused (UID) or compiled (GID) into the application processor and Secure Enclave during manufacturing. No software or firmware can read them directly; they can see only the results of encryption or decryption operations performed by dedicated AES engines implemented in silicon using the UID or GID as a key. Additionally, the Secure Enclave's UID and GID can only be used by the AES engine dedicated to the Secure Enclave. The UIDs are unique to each device and are not recorded by Apple or any of its suppliers. The GIDs are common to all processors in a class of devices (for example, all devices using the Apple A8 processor), and are used for non security-critical tasks such as when delivering system software during installation and restore. Integrating these keys into the silicon helps prevent them from being tampered with or bypassed, or accessed outside the AES engine. The UIDs and GIDs are also not available via JTAG or other debugging interfaces.

The UID allows data to be cryptographically tied to a particular device. For example, the key hierarchy protecting the file system includes the UID, so if the memory chips are physically moved from one device to another, the files are inaccessible. The UID is not related to any other identifier on the device.

Apart from the UID and GID, all other cryptographic keys are created by the system's random number generator (RNG) using an algorithm based on CTR_DRBG. System entropy is generated from timing variations during boot, and additionally from interrupt timing once the device has booted. Keys generated inside the Secure Enclave use its true hardware random number generator based on multiple ring oscillators post processed with CTR_DRBG.

Securely erasing saved keys is just as important as generating them. It's especially challenging to do so on flash storage, where wear-leveling might mean multiple copies of data need to be erased. To address this issue, iOS devices include a feature dedicated to secure data erasure called Effaceable Storage. This feature accesses the underlying storage technology (for example, NAND) to directly address and erase a small number of blocks at a very low level.

Erase all content and settings

The "Erase all content and settings" option in Settings obliterates all the keys in Effaceable Storage, rendering all user data on the device cryptographically inaccessible. Therefore, it's an ideal way to be sure all personal information is removed from a device before giving it to somebody else or returning it for service. Important: Do not use the "Erase all content and settings" option until the device has been backed up, as there is no way to recover the erased data.

File Data Protection

In addition to the hardware encryption features built into iOS devices, Apple uses a technology called Data Protection to further protect data stored in flash memory on the device. Data Protection allows the device to respond to common events such as incoming phone calls, but also enables a high level of encryption for user data. Key system apps, such as Messages, Mail, Calendar, Contacts, Photos, and Health data values use Data Protection by default, and third-party apps installed on iOS 7 or later receive this protection automatically.

Data Protection is implemented by constructing and managing a hierarchy of keys, and builds on the hardware encryption technologies built into each iOS device. Data Protection is controlled on a per-file basis by assigning each file to a class; accessibility is determined by whether the class keys have been unlocked.

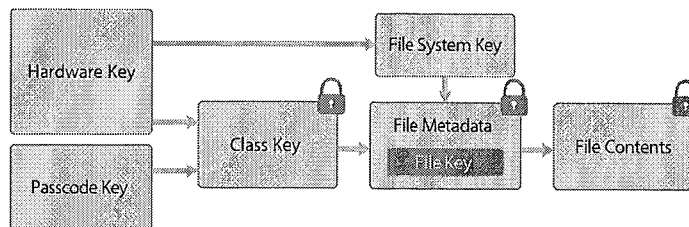
Architecture overview

Every time a file on the data partition is created, Data Protection creates a new 256-bit key (the “per-file” key) and gives it to the hardware AES engine, which uses the key to encrypt the file as it is written to flash memory using AES CBC mode. (On devices with an A8 processor, AES-XTS is used.) The initialization vector (IV) is calculated with the block offset into the file, encrypted with the SHA-1 hash of the per-file key.

The per-file key is wrapped with one of several class keys, depending on the circumstances under which the file should be accessible. Like all other wrappings, this is performed using NIST AES key wrapping, per RFC 3394. The wrapped per-file key is stored in the file’s metadata.

When a file is opened, its metadata is decrypted with the file system key, revealing the wrapped per-file key and a notation on which class protects it. The per-file key is unwrapped with the class key, then supplied to the hardware AES engine, which decrypts the file as it is read from flash memory. All wrapped file key handling occurs in the Secure Enclave; the file key is never directly exposed to the application processor. At boot, the Secure Enclave negotiates an ephemeral key with the AES engine. When the Secure Enclave unwraps a file’s keys, they are rewrapped with the ephemeral key and sent back to the application processor.

The metadata of all files in the file system is encrypted with a random key, which is created when iOS is first installed or when the device is wiped by a user. The file system key is stored in Effaceable Storage. Since it’s stored on the device, this key is not used to maintain the confidentiality of data; instead, it’s designed to be quickly erased on demand (by the user, with the “Erase all content and settings” option, or by a user or administrator issuing a remote wipe command from a mobile device management (MDM) server, Exchange ActiveSync, or iCloud). Erasing the key in this manner renders all files cryptographically inaccessible.



The content of a file is encrypted with a per-file key, which is wrapped with a class key and stored in a file's metadata, which is in turn encrypted with the file system key. The class key is protected with the hardware UID and, for some classes, the user's passcode. This hierarchy provides both flexibility and performance. For example, changing a file's class only requires rewrapping its per-file key, and a change of passcode just rewraps the class key.

Passcode considerations

If a long password that contains only numbers is entered, a numeric keypad is displayed at the Lock screen instead of the full keyboard. A longer numeric passcode may be easier to enter than a shorter alphanumeric passcode, while providing similar security.

Delays between passcode attempts

Attempts	Delay Enforced
1-4	none
5	1 minute
6	5 minutes
7-8	15 minutes
9	1 hour

Passcodes

By setting up a device passcode, the user automatically enables Data Protection. iOS supports six-digit, four-digit, and arbitrary-length alphanumeric passcodes. In addition to unlocking the device, a passcode provides entropy for certain encryption keys. This means an attacker in possession of a device can't get access to data in specific protection classes without the passcode.

The passcode is entangled with the device's UID, so brute-force attempts must be performed on the device under attack. A large iteration count is used to make each attempt slower. The iteration count is calibrated so that one attempt takes approximately 80 milliseconds. This means it would take more than 5½ years to try all combinations of a six-character alphanumeric passcode with lowercase letters and numbers.

The stronger the user passcode is, the stronger the encryption key becomes. Touch ID can be used to enhance this equation by enabling the user to establish a much stronger passcode than would otherwise be practical. This increases the effective amount of entropy protecting the encryption keys used for Data Protection, without adversely affecting the user experience of unlocking an iOS device multiple times throughout the day.

To further discourage brute-force passcode attacks, there are escalating time delays after the entry of an invalid passcode at the Lock screen. If Settings > Touch ID & Passcode > Erase Data is turned on, the device will automatically wipe after 10 consecutive incorrect attempts to enter the passcode. This setting is also available as an administrative policy through mobile device management (MDM) and Exchange ActiveSync, and can be set to a lower threshold.

On devices with an A7 or later A-series processor, the delays are enforced by the Secure Enclave. If the device is restarted during a timed delay, the delay is still enforced, with the timer starting over for the current period.

Data Protection classes

When a new file is created on an iOS device, it's assigned a class by the app that creates it. Each class uses different policies to determine when the data is accessible. The basic classes and policies are described in the following sections.

Complete Protection

(NSFileProtectionComplete): The class key is protected with a key derived from the user passcode and the device UID. Shortly after the user locks a device (10 seconds, if the Require Password setting is Immediately), the decrypted class key is discarded, rendering all data in this class inaccessible until the user enters the passcode again or unlocks the device using Touch ID.

Protected Unless Open

(`NSFileProtectionCompleteUnlessOpen`): Some files may need to be written while the device is locked. A good example of this is a mail attachment downloading in the background. This behavior is achieved by using asymmetric elliptic curve cryptography (ECDH over Curve25519). The usual per-file key is protected by a key derived using One-Pass Diffie-Hellman Key Agreement as described in NIST SP 800-56A.

The ephemeral public key for the agreement is stored alongside the wrapped per-file key. The KDF is Concatenation Key Derivation Function (Approved Alternative 1) as described in 5.8.1 of NIST SP 800-56A. `AlgorithmID` is omitted. `PartyUInfo` and `PartyVInfo` are the ephemeral and static public keys, respectively. SHA-256 is used as the hashing function. As soon as the file is closed, the per-file key is wiped from memory. To open the file again, the shared secret is re-created using the Protected Unless Open class's private key and the file's ephemeral public key; its hash is used to unwrap the per-file key, which is then used to decrypt the file.

Protected Until First User Authentication

(`NSFileProtectionCompleteUntilFirstUserAuthentication`): This class behaves in the same way as Complete Protection, except that the decrypted class key is not removed from memory when the device is locked. The protection in this class has similar properties to desktop full-volume encryption, and protects data from attacks that involve a reboot. This is the default class for all third-party app data not otherwise assigned to a Data Protection class.

No Protection

(`NSFileProtectionNone`): This class key is protected only with the UID, and is kept in Efaceable Storage. Since all the keys needed to decrypt files in this class are stored on the device, the encryption only affords the benefit of fast remote wipe. If a file is not assigned a Data Protection class, it is still stored in encrypted form (as is all data on an iOS device).

Keychain Data Protection

Many apps need to handle passwords and other short but sensitive bits of data, such as keys and login tokens. The iOS keychain provides a secure way to store these items.

The keychain is implemented as a SQLite database stored on the file system. There is only one database; the `securityd` daemon determines which keychain items each process or app can access. Keychain access APIs result in calls to the daemon, which queries the app's "keychain-access-groups," "application-identifier," and "application-group" entitlements. Rather than limiting access to a single process, access groups allow keychain items to be shared between apps.

Keychain items can only be shared between apps from the same developer. This is managed by requiring third-party apps to use access groups with a prefix allocated to them through the iOS Developer Program via application groups. The prefix requirement and application group uniqueness are enforced through code signing, Provisioning Profiles, and the iOS Developer Program.

Components of a keychain item

Along with the access group, each keychain item contains administrative metadata (such as “created” and “last updated” timestamps).

It also contains SHA-1 hashes of the attributes used to query for the item (such as the account and server name) to allow lookup without decrypting each item. And finally, it contains the encryption data, which includes the following:

- Version number
- Access control list (ACL) data
- Value indicating which protection class the item is in
- Per-item key wrapped with the protection class key
- Dictionary of attributes describing the item (as passed to `SecItemAdd`), encoded as a binary plist and encrypted with the per-item key

The encryption is AES 128 in GCM (Galois/Counter Mode); the access group is included in the attributes and protected by the GMAC tag calculated during encryption.

Keychain data is protected using a class structure similar to the one used in file Data Protection. These classes have behaviors equivalent to file Data Protection classes, but use distinct keys and are part of APIs that are named differently.

Availability	File Data Protection	Keychain Data Protection
When unlocked	<code>NSFileProtectionComplete</code>	<code>kSecAttrAccessibleWhenUnlocked</code>
While locked	<code>NSFileProtectionCompleteUnlessOpen</code>	N/A
After first unlock	<code>NSFileProtectionCompleteUntilFirstUserAuthentication</code>	<code>kSecAttrAccessibleAfterFirstUnlock</code>
Always	<code>NSFileProtectionNone</code>	<code>kSecAttrAccessibleAlways</code>
Passcode enabled	N/A	<code>kSecAttrAccessible-WhenPasscodeSetThisDeviceOnly</code>

Apps that utilize background refresh services can use `kSecAttrAccessibleAfterFirstUnlock` for keychain items that need to be accessed during background updates.

The class `kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly` behaves the same as `kSecAttrAccessibleWhenUnlocked`, however it is only available when the device is configured with a passcode. This class exists only in the system keybag; they do not sync to iCloud Keychain, are not backed up, and are not included in escrow keybags. If the passcode is removed or reset, the items are rendered useless by discarding the class keys.

Other keychain classes have a “This device only” counterpart, which is always protected with the UID when being copied from the device during a backup, rendering it useless if restored to a different device.

Apple has carefully balanced security and usability by choosing keychain classes that depend on the type of information being secured and when it’s needed by iOS. For example, a VPN certificate must always be available so the device keeps a continuous connection, but it’s classified as “non-migratory,” so it can’t be moved to another device.

For keychain items created by iOS, the following class protections are enforced:

Item	Accessible
Wi-Fi passwords	After first unlock
Mail accounts	After first unlock
Exchange accounts	After first unlock
VPN passwords	After first unlock
LDAP, CalDAV, CardDAV	After first unlock
Social network account tokens	After first unlock
Handoff advertisement encryption keys	After first unlock
iCloud token	After first unlock
Home sharing password	When unlocked
Find My iPhone token	Always
Voicemail	Always
iTunes backup	When unlocked, non-migratory
Safari passwords	When unlocked
Safari bookmarks	When unlocked
VPN certificates	Always, non-migratory
Bluetooth® keys	Always, non-migratory
Apple Push Notification service token	Always, non-migratory

iCloud certificates and private key	Always, non-migratory
iMessage keys	Always, non-migratory
Certificates and private keys installed by Configuration Profile	Always, non-migratory
SIM PIN	Always, non-migratory

Keychain access control

Keychains can use access control lists (ACLs) to set policies for accessibility and authentication requirements. Items can establish conditions that require user presence by specifying that they can't be accessed unless authenticated using Touch ID or by entering the device's passcode. ACLs are evaluated inside the Secure Enclave and are released to the kernel only if their specified constraints are met.

Access to Safari saved passwords

iOS apps can interact with keychain items saved by Safari for password autofill using the following two APIs:

- `SecRequestSharedWebCredential`
- `SecAddSharedWebCredential`

Access will be granted only if both the app developer and website administrator have given their approval, and the user has given consent. App developers express their intent to access Safari saved passwords by including an entitlement in their app. The entitlement lists the fully qualified domain names of associated websites. The websites must place a file on their server listing the unique app identifiers of apps they've approved. When an app with the `com.apple.developer.associated-domains` entitlement is installed, iOS makes a TLS request to each listed website, requesting the `file/apple-app-site-association`. If the file lists the app identifier of the app being installed, then iOS marks the website and app as having a trusted relationship. Only with a trusted relationship will calls to these two APIs result in a prompt to the user, who must agree before any passwords are released to the app, or are updated or deleted.

Keybags

The keys for both file and keychain Data Protection classes are collected and managed in keybags. iOS uses the following four keybags: system, backup, escrow, and iCloud Backup.

System keybag is where the wrapped class keys used in normal operation of the device are stored. For example, when a passcode is entered, the `NSFileProtectionComplete` key is loaded from the system keybag and unwrapped. It is a binary plist stored in the No Protection class, but whose contents are encrypted with a key held in Effaceable Storage. In order to give forward security to keybags, this key is wiped and regenerated each time a user changes their passcode. The `AppleKeyStore` kernel extension manages the system keybag, and can be queried regarding a device's lock state. It reports that the device is unlocked only if all the class keys in the system keybag are accessible, and have been unwrapped successfully.

Backup keybag is created when an encrypted backup is made by iTunes and stored on the computer to which the device is backed up. A new keybag is created with a new set of keys, and the backed-up data is re-encrypted to these new keys. As explained earlier, non-migratory keychain items remain wrapped with the UID-derived key, allowing them to be restored to the device they were originally backed up from, but rendering them inaccessible on a different device.

The keybag is protected with the password set in iTunes, run through 10,000 iterations of PBKDF2. Despite this large iteration count, there's no tie to a specific device, and therefore a brute-force attack parallelized across many computers could theoretically be attempted on the backup keybag. This threat can be mitigated with a sufficiently strong password.

If a user chooses not to encrypt an iTunes backup, the backup files are not encrypted regardless of their Data Protection class, but the keychain remains protected with a UID-derived key. This is why keychain items migrate to a new device only if a backup password is set.

Escrow keybag is used for iTunes syncing and MDM. This keybag allows iTunes to back up and sync without requiring the user to enter a passcode, and it allows an MDM server to remotely clear a user's passcode. It is stored on the computer that's used to sync with iTunes, or on the MDM server that manages the device.

The escrow keybag improves the user experience during device synchronization, which potentially requires access to all classes of data. When a passcode-locked device is first connected to iTunes, the user is prompted to enter a passcode. The device then creates an escrow keybag containing the same class keys used on the device, protected by a newly generated key. The escrow keybag and the key protecting it are split between the device and the host or server, with the data stored on the device in the Protected Until First User Authentication class. This is why the device passcode must be entered before the user backs up with iTunes for the first time after a reboot.

In the case of an OTA software update, the user is prompted for his or her passcode when initiating the update. This is used to securely create a One-time Unlock Token, which unlocks the system keybag after the update. This token cannot be generated without entering the user's passcode, and any previously generated token is invalidated if the user's passcode changed.

One-time Unlock Tokens are either for attended or unattended installation of a software update. They are encrypted with a key derived from the current value of a monotonic counter in the Secure Enclave, the UUID of the keybag, and the Secure Enclave's UID.

Incrementing the One-time Unlock Token counter in the SEP invalidates any existing token. The counter is incremented when a token is used, after the first unlock of a restarted device, when a software update is canceled (by the user or by the system), or when the policy timer for a token has expired.

The One-time Unlock Token for attended software updates expires after 20 minutes. This token is exported from the Secure Enclave and is written to effaceable storage. A policy timer increments the counter if the device has not rebooted within 20 minutes.

For unattended software updates, which is set when the user chooses "Install Later" when notified of the update, the application processor can keep the One-time Unlock Token alive in the Secure Enclave for up to 8 hours. After that time, a policy timer increments the counter.

iCloud Backup keybag is similar to the backup keybag. All the class keys in this keybag are asymmetric (using Curve25519, like the Protected Unless Open Data Protection class), so iCloud backups can be performed in the background. For all Data Protection classes except No Protection, the encrypted data is read from the device and sent to iCloud. The corresponding class keys are protected by iCloud keys. The keychain class keys are wrapped with a UID-derived key in the same way as an unencrypted iTunes backup. An asymmetric keybag is also used for the backup in the keychain recovery aspect of iCloud Keychain.

Security Certifications and programs

Cryptographic Validation (FIPS 140-2)

The cryptographic modules in iOS have been validated for compliance with U.S. Federal Information Processing Standards (FIPS) 140-2 Level 1 following each release since iOS 6. The cryptographic modules in iOS 9 are identical to those in iOS 8, but as with each release, Apple submits the modules for re-validation. This program validates the integrity of cryptographic operations for Apple apps and third-party apps that properly utilize iOS cryptographic services.

Common Criteria Certification (ISO 15408)

Apple has already begun pursuit of iOS certification under the Common Criteria Certification (CCC) program. The first two certifications currently active are against the Mobile Device Fundamental Protection Profile v2.0 (MDFPP2) and the VPN IPsecPP1.4 Client Protection Profile (VPNIPsecPP1.4). Apple has taken an active role within the International Technical Community (ITC) in developing currently unavailable Protection Profiles (PPs) focused on evaluating key mobile security technology. Apple continues to evaluate and pursue certifications against new and updated version of the PPs available today.

Commercial Solutions for Classified (CSfC)

Where applicable, Apple has also submitted the iOS platform and various services for inclusion in the Commercial Solutions for Classified (CSfC) Program Components List. Specifically, iOS for Mobile Platform and the IKEv2 client for the IPsec VPN Client (IKEv2 Always-On VPN only). As Apple platforms and services undergo Common Criteria Certifications, they will be submitted for inclusion under CSfC Program Component List as well.

Security Configuration Guides

Apple has collaborated with governments worldwide to develop guides that give instructions and recommendations for maintaining a more secure environment, also known as "device hardening." These guides provide defined and vetted information about how to configure and utilize features in iOS for enhanced protection.

For information on iOS security certifications, validations, and guidance, see <https://support.apple.com/kb/HT202739>.

App Security

Apps are among the most critical elements of a modern mobile security architecture. While apps provide amazing productivity benefits for users, they also have the potential to negatively impact system security, stability, and user data if they're not handled properly.

Because of this, iOS provides layers of protection to ensure that apps are signed and verified, and are sandboxed to protect user data. These elements provide a stable, secure platform for apps, enabling thousands of developers to deliver hundreds of thousands of apps on iOS without impacting system integrity. And users can access these apps on their iOS devices without undue fear of viruses, malware, or unauthorized attacks.

App code signing

Once the iOS kernel has started, it controls which user processes and apps can be run. To ensure that all apps come from a known and approved source and have not been tampered with, iOS requires that all executable code be signed using an Apple-issued certificate. Apps provided with the device, like Mail and Safari, are signed by Apple. Third-party apps must also be validated and signed using an Apple-issued certificate. Mandatory code signing extends the concept of chain of trust from the OS to apps, and prevents third-party apps from loading unsigned code resources or using self-modifying code.

In order to develop and install apps on iOS devices, developers must register with Apple and join the iOS Developer Program. The real-world identity of each developer, whether an individual or a business, is verified by Apple before their certificate is issued. This certificate enables developers to sign apps and submit them to the App Store for distribution. As a result, all apps in the App Store have been submitted by an identifiable person or organization, serving as a deterrent to the creation of malicious apps. They have also been reviewed by Apple to ensure they operate as described and don't contain obvious bugs or other problems. In addition to the technology already discussed, this curation process gives customers confidence in the quality of the apps they buy.

iOS allows developers to embed frameworks inside of their apps, which can be used by the app itself or by extensions embedded within the app. To protect the system and other apps from loading third-party code inside of their address space, the system will perform a code signature validation of all the dynamic libraries that a process links against at launch time. This verification is accomplished through the team identifier (Team ID), which is extracted from an Apple-issued certificate. A team identifier is a 10-character alphanumeric string; for example, 1A2B3C4D5F. A program may link against any platform library that ships with the system or any library with the same team identifier in its code signature as the main executable. Since the executables shipping as part of the system don't have a team identifier, they can only link against libraries that ship with the system itself.

Businesses also have the ability to write in-house apps for use within their organization and distribute them to their employees. Businesses and organizations can apply to the Apple Developer Enterprise Program (ADEP) with a D-U-N-S number. Apple approves applicants after verifying their identity and eligibility. Once an organization becomes a member of ADEP, it can register to obtain a Provisioning Profile that permits in-house apps to run on devices it authorizes. Users must have the Provisioning Profile installed in order to run the in-house apps. This ensures that only the organization's intended users are able to load the apps onto their iOS devices. Apps installed via MDM are implicitly trusted because the relationship between the organization and the device is already established. Otherwise, users have to approve the app's Provisioning Profile in Settings. Organizations can restrict users from approving apps from unknown developers. On first launch of any enterprise app, the device must receive positive confirmation from Apple that the app is allowed to run.

Unlike other mobile platforms, iOS does not allow users to install potentially malicious unsigned apps from websites, or run untrusted code. At runtime, code signature checks of all executable memory pages are made as they are loaded to ensure that an app has not been modified since it was installed or last updated.

Runtime process security

Once an app is verified to be from an approved source, iOS enforces security measures designed to prevent it from compromising other apps or the rest of the system.

All third-party apps are "sandboxed," so they are restricted from accessing files stored by other apps or from making changes to the device. This prevents apps from gathering or modifying information stored by other apps. Each app has a unique home directory for its files, which is randomly assigned when the app is installed. If a third-party app needs to access information other than its own, it does so only by using services explicitly provided by iOS.

System files and resources are also shielded from the user's apps. The majority of iOS runs as the non-privileged user "mobile," as do all third-party apps. The entire OS partition is mounted as read-only. Unnecessary tools, such as remote login services, aren't included in the system software, and APIs do not allow apps to escalate their own privileges to modify other apps or iOS itself.

Access by third-party apps to user information and features such as iCloud and extensibility is controlled using declared entitlements. Entitlements are key value pairs that are signed in to an app and allow authentication beyond runtime factors like unix user ID. Since entitlements are digitally signed, they cannot be changed. Entitlements are used extensively by system apps and daemons to perform specific privileged operations that would otherwise require the process to run as root. This greatly reduces the potential for privilege escalation by a compromised system application or daemon.

In addition, apps can only perform background processing through system-provided APIs. This enables apps to continue to function without degrading performance or dramatically impacting battery life.

Address space layout randomization (ASLR) protects against the exploitation of memory corruption bugs. Built-in apps use ASLR to ensure that all memory regions are randomized upon launch. Randomly arranging the memory addresses of executable code, system libraries, and related programming constructs reduces the likelihood of many sophisticated exploits. For example, a return-to-libc attack attempts to trick a device into executing malicious code by manipulating memory addresses of the stack and system libraries. Randomizing the placement of these makes the attack far more difficult to execute, especially across multiple devices. Xcode, the iOS development environment, automatically compiles third-party programs with ASLR support turned on.

Further protection is provided by iOS using ARM's Execute Never (XN) feature, which marks memory pages as non-executable. Memory pages marked as both writable and executable can be used only by apps under tightly controlled conditions: The kernel checks for the presence of the Apple-only dynamic code-signing entitlement. Even then, only a single mmap call can be made to request an executable and writable page, which is given a randomized address. Safari uses this functionality for its JavaScript JIT compiler.

Extensions

iOS allows apps to provide functionality to other apps by providing extensions. Extensions are special-purpose signed executable binaries, packaged within an app. The system automatically detects extensions at install time and makes them available to other apps using a matching system.

A system area that supports extensions is called an extension point. Each extension point provides APIs and enforces policies for that area. The system determines which extensions are available based on extension point-specific matching rules. The system automatically launches extension processes as needed and manages their lifetime. Entitlements can be used to restrict extension availability to particular system applications. For example, a Today view widget appears only in Notification Center, and a sharing extension is available only from the Sharing pane. The extension points are Today widgets, Share, Custom actions, Photo Editing, Document Provider, and Custom Keyboard.

Extensions run in their own address space. Communication between the extension and the app from which it was activated uses interprocess communications mediated by the system framework. They do not have access to each other's files or memory spaces. Extensions are designed to be isolated from each other, from their containing apps, and from the apps that use them. They are sandboxed like any other third-party app and have a container separate from the containing app's container. However, they share the same access to privacy controls as the container app. So if a user grants Contacts access to an app, this grant will be extended to the extensions that are embedded within the app, but not to the extensions activated by the app.

Custom keyboards are a special type of extensions since they are enabled by the user for the entire system. Once enabled, the extension will be used for any text field except the passcode input and any secure text view. For privacy reasons, custom keyboards run by default in a very restrictive sandbox that blocks access to the network, to services that perform network operations on behalf of a process, and to APIs that would allow the extension to exfiltrate typing data. Developers of custom keyboards can request that their extension have Open Access, which will let the system run the extension in the default sandbox after getting consent from the user.

For devices enrolled in mobile device management, document and keyboard extensions obey Managed Open In rules. For example, the MDM server can prevent a user from exporting a document from a managed app to an unmanaged Document Provider, or using an unmanaged keyboard with a managed app. Additionally, app developers can prevent the use of third-party keyboard extensions within their app.

App Groups

Apps and extensions owned by a given developer account can share content when configured to be part of an App Group. It is up to the developer to create the appropriate groups on the Apple Developer Portal and include the desired set of apps and extensions. Once configured to be part of an App Group, apps have access to the following:

- A shared on-disk container for storage, which will stay on the device as long as at least one app from the group is installed
- Shared preferences
- Shared keychain items

The Apple Developer Portal guarantees that App Group IDs are unique across the app ecosystem.

Data Protection in apps

The iOS Software Development Kit (SDK) offers a full suite of APIs that make it easy for third-party and in-house developers to adopt Data Protection and help ensure the highest level of protection in their apps. Data Protection is available for file and database APIs, including `NSFileManager`, `CoreData`, `NSData`, and `SQLite`.

The Mail app (including attachments), managed books, Safari bookmarks, app launch images, and location data are also stored encrypted with keys protected by the user's passcode on their device. Calendar (excluding attachments), Contacts, Reminders, Notes, Messages, and Photos implement Protected Until First User Authentication.

User-installed apps that do not opt-in to a specific Data Protection class receive Protected Until First User Authentication by default.

Accessories

The Made for iPhone, iPod touch, and iPad (MFi) licensing program provides vetted accessory manufacturers access to the iPod Accessories Protocol (iAP) and the necessary supporting hardware components.

When an MFi accessory communicates with an iOS device using a Lightning connector or via Bluetooth, the device asks the accessory to prove it has been authorized by Apple by responding with an Apple-provided certificate, which is verified by the device. The device then sends a challenge, which the accessory must answer with a signed response. This process is entirely handled by a custom integrated circuit that Apple provides to approved accessory manufacturers and is transparent to the accessory itself.

Accessories can request access to different transport methods and functionality; for example, access to digital audio streams over the Lightning cable, or location information provided over Bluetooth. An authentication IC ensures that only approved devices are granted full access to the device. If an accessory does not provide authentication, its access is limited to analog audio and a small subset of serial (UART) audio playback controls.

AirPlay also utilizes the authentication IC to verify that receivers have been approved by Apple. AirPlay audio and CarPlay video streams utilize the MFi-SAP (Secure Association Protocol), which encrypts communication between the accessory and device using AES-128 in CTR mode. Ephemeral keys are exchanged using ECDH key exchange (Curve25519) and signed using the authentication IC's 1024-bit RSA key as part of the Station-to-Station (STS) protocol.

HomeKit

HomeKit provides a home automation infrastructure that utilizes iCloud and iOS security to protect and synchronize private data without exposing it to Apple.

HomeKit identity

HomeKit identity and security are based on Ed25519 public-private key pairs. An Ed25519 key pair is generated on the iOS device for each user for HomeKit, which becomes his or her HomeKit identity. It is used to authenticate communication between iOS devices, and between iOS devices and accessories.

The keys are stored in Keychain and are included only in encrypted Keychain backups. The keys are synchronized between devices using iCloud Keychain.

Communication with HomeKit accessories

HomeKit accessories generate their own Ed25519 key pair for use in communicating with iOS devices. If the accessory is restored to factory settings, a new key pair is generated.

To establish a relationship between an iOS device and a HomeKit accessory, keys are exchanged using Secure Remote Password (3072-bit) protocol, utilizing an 8-digit code provided by the accessory's manufacturer and entered on the iOS device by the user, and then encrypted using ChaCha20-Poly1305 AEAD with HKDF-SHA-512-derived keys. The accessory's MFi certification is also verified during setup.

When the iOS device and the HomeKit accessory communicate during use, each authenticates the other utilizing the keys exchanged in the above process. Each session is established using the Station-to-Station protocol and is encrypted with HKDF-SHA-512 derived keys based on per-session Curve25519 keys. This applies to both IP-based and Bluetooth Low Energy accessories.

Local data storage

HomeKit stores data about the homes, accessories, scenes, and users on a user's iOS device. This stored data is encrypted using keys derived from the user's HomeKit identity keys, plus a random nonce. Additionally, HomeKit data is stored using Data Protection class Protected Until First User Authentication. HomeKit data is only backed up in encrypted backups, so, for example, unencrypted iTunes backups do not contain HomeKit data.

Data synchronization between devices and users

HomeKit data can be synchronized between a user's iOS devices using iCloud and iCloud Keychain. The HomeKit data is encrypted during the synchronization using keys derived from the user's HomeKit identity and random nonce. This data is handled as an opaque blob during synchronization. The most recent blob is stored in iCloud to enable synchronization, but it is not used for any other purposes. Because it is encrypted using keys that are available only on the user's iOS devices, its contents are inaccessible during transmission and iCloud storage.

HomeKit data is also synchronized between multiple users of the same home. This process uses authentication and encryption that is the same as that used between an iOS device and a HomeKit accessory. The authentication is based on Ed25519 public keys that are exchanged between the devices when a user is added to a home. After a new user is added to a home, every further communication is authenticated and encrypted using Station-to-Station protocol and per-session keys.

Only the user who initially created the home in HomeKit can add new users. His or her device configures the accessories with the public key of the new user so that the accessory can authenticate and accept commands from the new user. The process for configuring Apple TV for use with HomeKit uses the same authentication and encryption as when adding additional users, but is performed automatically if the user who created the home is signed in to iCloud on the Apple TV, and the Apple TV is in the home.

If a user does not have multiple devices, and does not grant additional users access to his or her home, no HomeKit data is synchronized to iCloud.

Home data and apps

Access to home data by apps is controlled by the user's Privacy settings. Users are asked to grant access when apps request home data, similar to Contacts, Photos, and other iOS data sources. If the user approves, apps have access to the names of rooms, names of accessories, and which room each accessory is in, and other information as detailed in the HomeKit developer documentation.

Siri

Siri can be used to query and control accessories, and to activate scenes. Minimal information about the configuration of the home is provided anonymously to Siri, as described in the Siri section of this paper, to provide names of rooms, accessories, and scenes that are necessary for command recognition.

iCloud remote access for HomeKit accessories

HomeKit accessories can connect directly with iCloud to enable iOS devices to control the accessory when Bluetooth or Wi-Fi communication isn't available.

iCloud Remote access has been carefully designed so that accessories can be controlled and send notifications without revealing to Apple what the accessories are, or what commands and notifications are being sent. HomeKit does not send information about the home over iCloud Remote access.

When a user sends a command using iCloud remote access, the accessory and iOS device are mutually authenticated and data is encrypted using the same procedure described for local connections. The contents of the communications are encrypted and not visible to Apple. The addressing through iCloud is based on the iCloud identifiers registered during the setup process.

Accessories that support iCloud remote access are provisioned during the accessory's setup process. The provisioning process begins with the user signing in to iCloud. Next, the iOS device asks the accessory to sign a challenge using the Apple Authentication Coprocessor that is built into all Built for HomeKit accessories. The accessory also generates prime256v1 elliptic curve keys, and the public key is sent to the iOS device along with the signed challenge and the X.509 certificate of the authentication coprocessor. These are used to request a certificate for the accessory from the iCloud provisioning server. The certificate is stored by the accessory, but it does not contain any identifying information about the accessory, other than it has been granted access to HomeKit iCloud remote access. The iOS device that is conducting the provisioning also sends a bag to the accessory, which contains the URLs and other information needed to connect to the iCloud remote access server. This information is not specific to any user or accessory.

Each accessory registers a list of allowed users with the iCloud remote access server. These users have been granted the ability to control the accessory by the person who added the accessory to the home. Users are granted an identifier by the iCloud server and can be mapped to an iCloud account for the purpose of delivering notification messages and responses from the accessories. Similarly, accessories have iCloud-issued identifiers, but these identifiers are opaque and don't reveal any information about the accessory itself.

When an accessory connects to the HomeKit iCloud remote access server, it presents its certificate and a pass. The pass is obtained from a different iCloud server and it is not unique for each accessory. When an accessory requests a pass, it includes its manufacturer, model, and firmware version in its request. No user-identifying or home-identifying information is sent in this request. The connection to the pass server is not authenticated, in order to help protect privacy.

Accessories connect to the iCloud remote access server using HTTP/2, secured using TLS 1.2 with AES-128-GCM and SHA-256. The accessory keeps its connection to the iCloud remote access server open so that it can receive incoming messages and send responses and outgoing notifications to iOS devices.

HealthKit

The HealthKit framework provides a common database that apps can use to store and access fitness and health data with permission of the user. HealthKit also works directly with health and fitness devices, such as compatible Bluetooth LE heart rate monitors and the motion coprocessor built into many iOS devices.

Health data

HealthKit uses a database to store the user's health data, such as height, weight, distance walked, blood pressure, and so on. This database is stored in Data Protection class Complete Protection, which means it is accessible only after a user enters his or her passcode or uses Touch ID to unlock the device.

Another database stores operational data, such as access tables for apps, names of devices connected to HealthKit, and scheduling information used to launch apps when new data is available. This database is stored in Data Protection class Protected Until First User Authentication.

Temporary journal files store health records that are generated when the device is locked, such as when the user is exercising. These are stored in Data Protection class Protected Unless Open. When the device is unlocked, they are imported into the primary health databases, then deleted when the merge is completed.

Health data is not shared via iCloud or synced between devices. Health databases are included in encrypted device backups to iCloud or iTunes. Health data is not included in unencrypted iTunes backups.

Data Integrity

Data stored in the database includes metadata to track the provenance of each data record. This metadata includes an application identifier that identifies which app stored the record. Additionally, an optional metadata item can contain a digitally signed copy of the record. This is intended to provide data integrity for records generated by a trusted device. The format used for the digital signature is the Cryptographic Message Syntax (CMS) specified in IETF RFC 5652.

Access by third-party apps

Access to the HealthKit API is controlled with entitlements, and apps must conform to restrictions about how the data is used. For example, apps are not allowed to utilize health data for advertising. Apps are also required to provide users with a privacy policy that details its use of health data.

Access to health data by apps is controlled by the user's Privacy settings. Users are asked to grant access when apps request access to health data, similar to Contacts, Photos, and other iOS data sources. However, with health data, apps are granted separate access for reading and writing data, as well as separate access for each type of health data. Users can view, and revoke, permissions they've granted for accessing health data in the Sources tab of the Health app.

If granted permission to write data, apps can also read the data they write. If granted the permission to read data, they can read data written by all sources. However, apps can't determine access granted to other apps. In addition, apps can't conclusively tell if they have been granted read access to health data. When an app does not have read access, all queries return no data—the same response as an empty database would return. This prevents apps from inferring the user's health status by learning which types of data the user is tracking.

Medical ID

The Health app gives users the option of filling out a Medical ID form with information that could be important during a medical emergency. The information is entered or updated manually and is not synchronized with the information in the health databases.

The Medical ID information is viewed by tapping the Emergency button on the Lock screen. The information is stored on the device using Data Protection class No Protection so that it is accessible without having to enter the device passcode. Medical ID is an optional feature that enables users to decide how to balance both safety and privacy concerns.

Apple Watch

Apple Watch uses the security features and technology built for iOS to help protect data on the device, as well as communications with its paired iPhone and the Internet. This includes technologies such as Data Protection and keychain access control. The user's passcode is also entangled with the device UID to create encryption keys.

Pairing Apple Watch with iPhone is secured using an out-of-band (OOB) process to exchange public keys, followed by the BTLE link shared secret. Apple Watch displays an animated pattern, which is captured by the camera on iPhone. The pattern contains an encoded secret that is used for BTLE 4.1 out-of-band pairing. Standard BTLE Passkey Entry is used as a fallback pairing method, if necessary.

Once the BTLE session is established, Apple Watch and iPhone exchange keys using a process adapted from IDS, as described in the iMessage section of this paper. Once keys have been exchanged, the Bluetooth session key is discarded, and all communications

between Apple Watch and iPhone are encrypted using IDS, with the encrypted BTLE and Wi-Fi links providing a secondary encryption layer. Key rolling is utilized at 15-minute intervals to limit the exposure window, should traffic be compromised.

To support apps that need streaming data, encryption is provided using methods described in the FaceTime section of this paper, utilizing the IDS service provided by the paired iPhone.

Apple Watch implements hardware-encrypted storage and class-based protection of files and keychain items, as described in the Data Protection section of this paper. Access-controlled keybags for keychain items are also used. Keys used for communication between the watch and iPhone are also secured using class-based protection.

When Apple Watch is not within Bluetooth range, Wi-Fi can be used instead. Apple Watch will not join Wi-Fi networks unless the credentials to do so are present on the paired iPhone, which provides the list of known networks to the watch automatically.

Apple Watch can be manually locked by holding down the side button. Additionally, motion heuristics are used to attempt to automatically lock the device shortly after it's removed from the wrist. When locked, Apple Pay can't be used. If the automatic locking provided by wrist detection is turned off in settings, Apple Pay is disabled. Wrist detection is turned off using the Apple Watch app on iPhone. This setting can also be enforced using mobile device management.

The paired iPhone can also unlock the watch, provided the watch is being worn. This is accomplished by establishing a connection authenticated by the keys established during pairing. iPhone sends the key, which the watch uses to unlock its Data Protection keys. The watch passcode is not known to iPhone nor is it transmitted. This feature can be turned off using the Apple Watch app on iPhone.

Apple Watch can be paired with only one iPhone at a time. Pairing with a new iPhone automatically erases all content and data from Apple Watch.

Enabling Find My Phone on the paired iPhone also enables Activation Lock on Apple Watch. Activation Lock makes it harder for anyone to use or sell an Apple Watch that has been lost or stolen. Activation Lock requires the user's Apple ID and password to unpair, erase, or reactivate an Apple Watch.

Network Security

In addition to the built-in safeguards Apple uses to protect data stored on iOS devices, there are many network security measures that organizations can take to keep information secure as it travels to and from an iOS device.

Mobile users must be able to access corporate networks from anywhere in the world, so it's important to ensure that they are authorized and their data is protected during transmission. iOS uses—and provides developer access to—standard networking protocols for authenticated, authorized, and encrypted communications. To accomplish these security objectives, iOS integrates proven technologies and the latest standards for both Wi-Fi and cellular data network connections.

On other platforms, firewall software is needed to protect open communication ports against intrusion. Because iOS achieves a reduced attack surface by limiting listening ports and removing unnecessary network utilities such as telnet, shells, or a web server, no additional firewall software is needed on iOS devices.

TLS

iOS supports Transport Layer Security (TLS v1.0, TLS v1.1, TLS v1.2) and DTLS. Safari, Calendar, Mail, and other Internet apps automatically use these mechanisms to enable an encrypted communication channel between the device and network services. High-level APIs (such as CFNetwork) make it easy for developers to adopt TLS in their apps, while low-level APIs (SecureTransport) provide fine-grained control. By default, CFNetwork disallows SSLv3, and apps that use WebKit (such as Safari) are prohibited from making an SSLv3 connection.

App Transport Security

App Transport Security provides default connection requirements so that apps adhere to best practices for secure connections when using NSURLConnection, CFURL, or NSURLSession APIs.

Servers must support a minimum of TLS 1.2, forward secrecy, and certificates must be valid and signed using SHA-256 or better with a minimum of a 2048-bit RSA key or 256-bit elliptic curve key.

Network connections that don't meet these requirements will fail, unless the app overrides App Transport Security. Invalid certificates always result in a hard failure and no connection. App Transport Security is automatically applied to apps that are compiled for iOS 9.

VPN

Secure network services like virtual private networking typically require minimal setup and configuration to work with iOS devices. iOS devices work with VPN servers that support the following protocols and authentication methods:

- IKEv2/IPSec with authentication by shared secret, RSA Certificates, ECDSA Certificates, EAP-MSCHAPv2, or EAP-TLS.
- Pulse Secure, Cisco, Aruba Networks, SonicWALL, Check Point, Palo Alto Networks, Open VPN, AirWatch, MobileIron, NetMotion Wireless, and F5 Networks SSL-VPN using the appropriate client app from the App Store.
- Cisco IPSec with user authentication by Password, RSA SecurID or CRYPTOCARD, and machine authentication by shared secret and certificates.
- L2TP/IPSec with user authentication by MS-CHAPV2 Password, RSA SecurID or CRYPTOCARD, and machine authentication by shared secret.
- PPTP with user authentication by MS-CHAPV2 Password and RSA SecurID or CRYPTOCARD is supported, but not recommended.

iOS supports VPN On Demand for networks that use certificate-based authentication. IT policies specify which domains require a VPN connection by using a configuration profile.

iOS also supports Per App VPN support, facilitating VPN connections on a much more granular basis. Mobile device management (MDM) can specify a connection for each managed app and/or specific domains in Safari. This helps ensure that secure data always goes to and from the corporate network—and that a user's personal data does not.

iOS supports Always-on VPN, which can be configured for devices managed via MDM and supervised using Apple Configurator or the Device Enrollment Program. This eliminates the need for users to turn on VPN to enable protection when connecting to cellular and Wi-Fi networks. Always-on VPN gives an organization full control over device traffic by tunneling all IP traffic back to the organization. The default tunneling protocol, IKEv2, secures traffic transmission with data encryption. The organization can now monitor and filter traffic to and from its devices, secure data within its network, and restrict device access to the Internet.

Wi-Fi

iOS supports industry-standard Wi-Fi protocols, including WPA2 Enterprise, to provide authenticated access to wireless corporate networks. WPA2 Enterprise uses 128-bit AES encryption, giving users the highest level of assurance that their data remains protected when sending and receiving communications over a Wi-Fi network connection. With support for 802.1X, iOS devices can be integrated into a broad range of RADIUS authentication environments. 802.1X wireless authentication methods supported on iPhone and iPad include EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, PEAPv0, PEAPv1, and LEAP.

iOS uses a randomized Media Access Control (MAC) address when conducting Preferred Network Offload (PNO) scans when a device is not associated with a Wi-Fi network and its processor is asleep. A device's processor goes to sleep shortly after the screen is turned off. PNO scans are run to determine if a user can connect to a preferred Wi-Fi network to conduct activity such as wirelessly syncing with iTunes.

iOS also uses a randomized MAC address when conducting enhanced Preferred Network Offload (ePNO) scans when a device is not associated with a Wi-Fi network or its processor is asleep. ePNO scans are run when a device uses Location Services for apps which use geofences, such as location-based reminders that determine whether the device is near a specific location.

Because a device's MAC address now changes when it's not connected to a Wi-Fi network, it can't be used to persistently track a device by passive observers of Wi-Fi traffic, even when the device is connected to a cellular network.

We've worked with Wi-Fi manufacturers to let them know that background scans use a randomized MAC address, and that neither Apple nor manufacturers can predict these randomized MAC addresses.

Wi-Fi MAC address randomization is not supported on iPhone 4s.

Bluetooth

Bluetooth support in iOS has been designed to provide useful functionality without unnecessary increased access to private data. iOS devices support Encryption Mode 3, Security Mode 4, and Service Level 1 connections. iOS supports the following Bluetooth profiles:

- Hands-Free Profile (HFP 1.5)
- Phone Book Access Profile (PBAP)
- Advanced Audio Distribution Profile (A2DP)
- Audio/Video Remote Control Profile (AVRCP)
- Personal Area Network Profile (PAN)
- Human Interface Device Profile (HID)

Support for these profiles varies by device. For more information, see <https://support.apple.com/kb/ht3647>.

Single Sign-on

iOS supports authentication to enterprise networks through Single Sign-on (SSO). SSO works with Kerberos-based networks to authenticate users to services they are authorized to access. SSO can be used for a range of network activities, from secure Safari sessions to third-party apps.

iOS SSO utilizes SPNEGO tokens and the HTTP Negotiate protocol to work with Kerberos-based authentication gateways and Windows Integrated Authentication systems that support Kerberos tickets. Certificate-based authentication is also supported. SSO support is based on the open source Heimdal project.

The following encryption types are supported:

- AES128-CTS-HMAC-SHA1-96
- AES256-CTS-HMAC-SHA1-96
- DES3-CBC-SHA1
- ARCFOUR-HMAC-MD5

Safari supports SSO, and third-party apps that use standard iOS networking APIs can also be configured to use it. To configure SSO, iOS supports a configuration profile payload that allows MDM servers to push down the necessary settings. This includes setting the user principal name (that is, the Active Directory user account) and Kerberos realm settings, as well as configuring which apps and/or Safari web URLs should be allowed to use SSO.

AirDrop security

iOS devices that support AirDrop use Bluetooth Low Energy (BLE) and Apple-created peer-to-peer Wi-Fi technology to send files and information to nearby devices, including AirDrop-capable Mac computers running OS X Yosemite or later. The Wi-Fi radio is used to communicate directly between devices without using any Internet connection or Wi-Fi Access Point.

When a user enables AirDrop, a 2048-bit RSA identity is stored on the device. Additionally, an AirDrop identity hash is created based on the email addresses and phone numbers associated with the user's Apple ID.

When a user chooses AirDrop as the method for sharing an item, the device emits an AirDrop signal over Bluetooth Low Energy. Other devices that are awake, in close proximity, and have AirDrop turned on detect the signal and respond with a shortened version of their owner's identity hash.

AirDrop is set to share with Contacts Only by default. Users can also choose if they want to be able to use AirDrop to share with Everyone or turn off the feature entirely. In Contacts Only mode, the received identity hashes are compared with hashes of people in the initiator's Contacts app. If a match is found, the sending device creates a peer-to-peer Wi-Fi network and advertises an AirDrop connection using Bonjour. Using this connection, the receiving devices send their full identity hashes to the initiator. If the full hash still matches Contacts, the recipient's first name and photo (if present in Contacts) are displayed in the AirDrop sharing sheet.

When using AirDrop, the sending user selects who they want to share with. The sending device initiates an encrypted (TLS) connection with the receiving device, which exchanges their iCloud identity certificates. The identity in the certificates is verified against each user's Contacts app. Then the receiving user is asked to accept the incoming transfer from the identified person or device. If multiple recipients have been selected, this process is repeated for each destination.

In the Everyone mode, the same process is used but if a match in Contacts is not found, the receiving devices are shown in the AirDrop sending sheet with a silhouette and with the device's name, as defined in Settings > General > About > Name.

Organizations can restrict the use of AirDrop for devices or apps being managed by a mobile device management solution.

Apple Pay

With Apple Pay, users can use supported iOS devices and Apple Watch to pay in an easy, secure, and private way. It's simple for users, and it's built with integrated security in both hardware and software.

Apple Pay is also designed to protect the user's personal information. Apple Pay doesn't collect any transaction information that can be tied back to the user. Payment transactions are between the user, the merchant, and the card issuer.

Apple Pay components

Secure Element: The Secure Element is an industry-standard, certified chip running the Java Card platform, which is compliant with financial industry requirements for electronic payments.

NFC controller: The NFC controller handles Near Field Communication protocols and routes communication between the application processor and the Secure Element, and between the Secure Element and the point-of-sale terminal.

Wallet: Wallet is used to add and manage credit, debit, rewards, and store cards and to make payments with Apple Pay. Users can view their cards and additional information about their card issuer, their card issuer's privacy policy, recent transactions, and more in Wallet. Users can also add cards to Apple Pay in Setup Assistant and Settings.

Secure Enclave: On iPhone and iPad, the Secure Enclave manages the authentication process and enables a payment transaction to proceed. It stores fingerprint data for Touch ID.

On Apple Watch, the device must be unlocked, and the user must double-click the side button. The double-click is detected and passed to the Secure Element directly without going through the application processor.

Apple Pay Servers: The Apple Pay Servers manage the state of credit and debit cards in Wallet and the Device Account Numbers stored in the Secure Element. They communicate both with the device and with the payment network servers. The Apple Pay Servers are also responsible for re-encrypting payment credentials for payments within apps.

How Apple Pay uses the Secure Element

The Secure Element hosts a specially designed applet to manage Apple Pay. It also includes payment applets certified by the payment networks. Credit or debit card data is sent from the payment network or card issuer encrypted to these payment applets using keys that are known only to the payment network and the payment applets' security domain. This data is stored within these payment applets and protected using the Secure Element's security features. During a transaction, the terminal communicates directly with the Secure Element through the Near Field Communication (NFC) controller over a dedicated hardware bus.

How Apple Pay uses the NFC controller

As the gateway to the Secure Element, the NFC controller ensures that all contactless payment transactions are conducted using a point-of-sale terminal that is in close proximity with the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions.

Once payment is authorized by the card holder using Touch ID or passcode, or on an unlocked Apple Watch by double-clicking the side button, contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field. Consequently, payment authorization details for contactless transactions are contained to the local NFC field and are never exposed to the application processor. In contrast, payment authorization details for payments within apps are routed to the application processor, but only after encryption by the Secure Element to the Apple Pay Server.

Credit and debit card provisioning

When a user adds a credit or debit card (including store cards) to Apple Pay, Apple securely sends the card information, along with other information about user's account and device, to the card issuer. Using this information, the card issuer will determine whether to approve adding the card to Apple Pay.

Apple Pay uses three server-side calls to send and receive communication with the card issuer or network as part of the card provisioning process: *Required Fields*, *Check Card*, and *Link and Provision*. The card issuer or network uses these calls to verify, approve, and add cards to Apple Pay. These client-server sessions are encrypted using SSL.

Full card numbers are not stored on the device or on Apple servers. Instead, a unique Device Account Number is created, encrypted, and then stored in the Secure Element. This unique Device Account Number is encrypted in such a way that Apple can't access it. The Device Account Number is unique and different from usual credit or debit card numbers, the card issuer can prevent its use on a magnetic stripe card, over the phone, or on websites. The Device Account Number in the Secure Element is isolated from iOS and WatchOS, is never stored on Apple Pay Servers, and is never backed up to iCloud.

Cards for use with Apple Watch are provisioned for Apple Pay using the Apple Watch app on iPhone. Provisioning a card for Apple Watch requires that the watch be within Bluetooth communications range. Cards are specifically enrolled for use with Apple Watch and have their own Device Account Numbers, which are stored within the Secure Element on the Apple Watch.

There are two ways to provision a credit or debit card into Apple Pay:

- Adding a credit or debit card manually to Apple Pay
- Adding credit or debit cards on file from an iTunes Store account to Apple Pay

Adding a credit or debit card manually to Apple Pay

To add a card manually, including store cards, the name, credit card number, expiration date, and CVV are used to facilitate the provisioning process. From within Settings, the Wallet app, or the Apple Watch app, users can enter that information by typing, or using the iSight camera. When the camera captures the card information, Apple attempts to populate the name, card number, and expiration date. The photo is never saved to the device or stored in the photo library. Once all the fields are filled in, the Check Card process verifies the fields other than the CVV. They are encrypted and sent to the Apple Pay Server.

If a terms and conditions ID is returned with the Check Card process, Apple downloads and displays the terms and conditions of the card issuer to the user. If the user accepts the terms and conditions, Apple sends the ID of the terms that were accepted, as well as the CVV to the Link and Provision process. Additionally, as part of the Link and Provision process, Apple shares information from the device with the card issuer or network, like information about your iTunes and App Store account activity (for example, whether you have a long history of transactions within iTunes), information about your device (for example, phone number, name, and model of your device plus any companion iOS device necessary to set up Apple Pay), as well as your approximate location at the time you add your card (if you have Location Services enabled). Using this information, the card issuer will determine whether to approve adding the card to Apple Pay.

As the result of the Link and Provision process, two things occur:

- The device begins to download the Wallet pass file representing the credit or debit card.
- The device begins to bind the card to the Secure Element.

The pass file contains URLs to download card art, metadata about the card such as contact information, the related issuer's app, and supported features. It also contains the pass state, which includes information such as whether the personalizing of the Secure Element has completed, whether the card is currently suspended by the card issuer, or whether additional verification is required before the card will be able to make payments with Apple Pay.

Adding credit or debit cards from an iTunes Store account to Apple Pay

For a credit or debit card on file with iTunes, the user may be required to re-enter their Apple ID password. The card number is retrieved from iTunes and the Check Card process is initiated. If the card is eligible for Apple Pay, the device will download and display terms and conditions, then send along the term's ID and the card security code to the Link and Provision process. Additional verification may occur for iTunes account cards on file.

Adding credit or debit cards from a card issuer's app

When the app is registered for use with Apple Pay, keys are established for the app and the merchant's server. These keys are used to encrypt the card information that's sent to the merchant, which prevents the information from being read by the iOS device. The provisioning flow is similar to that used for manually added cards, described above, except that one-time passwords are used in lieu of the CVV.

Additional verification

A card issuer can decide whether a credit or debit card requires additional verification. Depending on what is offered by the card issuer, the user may be able to choose between different options for additional verification, such as a text message, email, customer service call, or a method in an approved third-party app to complete the verification. For text messages or email, the user selects from contact information the issuer has on file. A code will be sent, which the user will need to enter into Wallet, Settings, or the Apple Watch app. For customer service or verification using an app, the issuer performs their own communication process.

Payment authorization

The Secure Element will only allow a payment to be made after it receives authorization from the Secure Enclave, confirming the user has authenticated with Touch ID or the device passcode. Touch ID is the default method if available but the passcode can be used at any time instead of Touch ID. A passcode is automatically offered after three unsuccessful attempts to match a fingerprint and after five unsuccessful attempts, the passcode is required. A passcode is also required when Touch ID is not configured or not enabled for Apple Pay.

Communication between the Secure Enclave and the Secure Element takes place over a serial interface, with the Secure Element connected to the NFC controller, which in turn is connected to the application processor. Even though not directly connected, the Secure Enclave and Secure Element can communicate securely using a shared pairing key that is provisioned during the manufacturing process. The encryption and authentication of the communication is based on AES, with cryptographic nonces used by both sides to protect against replay attacks. The pairing key is generated inside the Secure Enclave from its UID key and the Secure Element's unique identifier. The pairing key is then securely transferred from the Secure Enclave to a hardware security module (HSM) in the factory, which has the key material required to then inject the pairing key into the Secure Element.

When the user authorizes a transaction, the Secure Enclave sends signed data about the type of authentication and details about the type of transaction (contactless or within apps) to the Secure Element, tied to an Authorization Random (AR) value. The AR is generated in the Secure Enclave when a user first provisions a credit card and is persisted while Apple Pay is enabled, protected by the Secure Enclave's encryption and anti-rollback mechanism. It is securely delivered to the Secure Element via the pairing key. On receipt of a new AR value, the Secure Element marks any previously added cards as deleted.

Credit and debit cards added to the Secure Element can only be used if the Secure Element is presented with authorization using the same pairing key and AR value from when the card was added. This allows iOS to instruct the Secure Enclave to render cards unusable by marking its copy of the AR as invalid under the following scenarios:

When the passcode is disabled.

- The user logs out of iCloud.
- The user selects Erase All Content and Settings.
- The device is restored from recovery mode.

With Apple Watch, cards are marked as invalid when:

- The watch's passcode is disabled.
- The watch is unpaired from iPhone.
- Wrist detection is turned off.

Using the pairing key and its copy of the current AR value, the Secure Element verifies the authorization received from the Secure Enclave before enabling the payment applet for a contactless payment. This process also applies when retrieving encrypted payment data from a payment applet for transactions within apps.

Transaction-specific dynamic security code

All payment transactions originating from the payment applets include a transaction-specific dynamic security code along with a Device Account Number. This one-time code is computed using a counter that is incremented for each new transaction, and a key that's provisioned in the payment applet during personalization and is known by the payment network and/or the card issuer. Depending on the payment scheme, other data may also be used in the calculation of these codes, including the following:

- A random number generated by the payment applet
- Another random number generated by the terminal—in the case of an NFC transaction or
- Another random number generated by the server—in the case of transactions within apps

These security codes are provided to the payment network and the card issuer, which allows them to verify each transaction. The length of these security codes may vary based on the type of transaction being done.

Contactless payments with Apple Pay

If iPhone is on and detects an NFC field, it will present the user with the relevant credit or debit card, or the default card, which is managed in Settings. The user can also go to the Wallet app and choose a credit or debit card, or when the device is locked, double-click the Home button.

Next, the user must authenticate using Touch ID or their passcode before payment information is transmitted. When Apple Watch is unlocked, double-clicking the side button activates the default card for payment. No payment information is sent without user authentication.

Once the user authenticates, the Device Account Number and a transaction-specific dynamic security code are used when processing the payment. Neither Apple nor a user's device sends the full actual credit or debit card numbers to merchants. Apple may receive anonymous transaction information such as the approximate time and location of the transaction, which helps improve Apple Pay and other Apple products and services.

Paying with Apple Pay within apps

Apple Pay can also be used to make payments within iOS apps. When users pay in apps using Apple Pay, Apple receives encrypted transaction information and re-encrypts it with a merchant-specific key before it's sent to the merchant. Apple Pay retains anonymous transaction information such as approximate purchase amount. This information can't be tied back to the user and never includes what the user is buying.

When an app initiates an Apple Pay payment transaction, the Apple Pay Servers receive the encrypted transaction from the device prior to the merchant receiving it. The Apple Pay Servers then re-encrypt it with a merchant-specific key before relaying the transaction to the merchant.

When an app requests a payment, it calls an API to determine if the device supports Apple Pay and if the user has credit or debit cards that can make payments on a payment network accepted by the merchant. The app requests any pieces of information it needs to process and fulfill the transaction, such as the billing and shipping address, and contact information. The app then asks iOS to present the Apple Pay sheet, which requests information for the app, as well as other necessary information, such as the card to use.

At this time, the app is presented with city, state, and zip code information to calculate the final shipping cost. The full set of requested information isn't provided to the app until the user authorizes the payment with Touch ID or the device passcode. Once the payment is authorized, the information presented in the Apple Pay sheet will be transferred to the merchant.

When the user authorizes the payment, a call is made to the Apple Pay Servers to obtain a cryptographic nonce, which is similar to the value returned by the NFC terminal used for in-store transactions. The nonce, along with other transaction data, is passed to the Secure Element to generate a payment credential that will be encrypted with an Apple key. When the encrypted payment credential comes out of the Secure Element, it's passed to the Apple Pay Servers, which decrypt the credential, verify the nonce in the credential against the nonce sent by the Secure Element, and re-encrypt the payment credential with the merchant key associated with the Merchant ID. It's then returned to the device, which hands it back to the app via the API. The app then passes it along to the merchant system for processing. The merchant can then decrypt the payment credential with its private key for processing. This, together with the signature from Apple's servers, allows the merchant to verify that the transaction was intended for this particular merchant.

The APIs require an entitlement that specifies the supported merchant IDs. An app can also include additional data to send to the Secure Element to be signed, such as an order number or customer identity, ensuring the transaction can't be diverted to a different customer. This is accomplished by the app developer. The app developer is able to specify `applicationData` on the `PKPaymentRequest`. A hash of this data is included in the encrypted payment data. The merchant is then responsible for verifying that their `applicationData` hash matches what's included in the payment data.

Rewards cards

As of iOS 9, Apple Pay supports the Value Added Service (VAS) protocol for transmitting merchant rewards cards to compatible NFC terminals. The VAS protocol can be implemented on merchant terminals and uses NFC to communicate with supported Apple devices. The VAS protocol works over a short distance and is used to provide complementary services, such as transmission of rewards card information, as part of an Apple Pay transaction.

The NFC terminal initiates receiving the card information by sending a request for a card. If the user has a card with the store's identifier, the user is asked to authorize its use. If the merchant supports encryption, the card information, a timestamp, and a single-use random ECDH P-256 key is used with the merchant's public key to derive an encryption key for the card data, which is sent to the terminal. If the merchant does not support encryption, the user is asked to re-present the device to the terminal before the rewards card information is sent.

Suspending, removing, and erasing cards

Users can suspend Apple Pay on iPhone and iPad by placing their devices in Lost Mode using Find My iPhone. Users also have the ability to remove and erase their cards from Apple Pay using Find My iPhone, iCloud Settings, or directly on their devices using Wallet. On Apple Watch, cards can be removed using iCloud settings, the Apple Watch app on iPhone, or directly on the watch. The ability to make payments using cards on the device will be suspended or removed from Apple Pay by the card issuer or respective payment network even if the device is offline and not connected to a cellular or Wi-Fi network. Users can also call their card issuer to suspend or remove cards from Apple Pay.

Additionally, when a user erases the entire device using "Erase All Content and Settings," using Find My iPhone, or restoring their device using recovery mode, iOS will instruct the Secure Element to mark all cards as deleted. This has the effect of immediately changing the cards to an unusable state until the Apple Pay Servers can be contacted to fully erase the cards from the Secure Element. Independently, the Secure Enclave marks the AR as invalid, so that further payment authorizations for previously enrolled cards aren't possible. When the device is online, it attempts to contact the Apple Pay Servers to ensure all cards in the Secure Element are erased.

Internet Services

Creating strong Apple ID passwords

Apple IDs are used to connect to a number of services including iCloud, FaceTime, and iMessage. To help users create strong passwords, all new accounts must contain the following password attributes:

- At least eight characters
- At least one letter
- At least one uppercase letter
- At least one number
- No more than three consecutive identical characters
- Not the same as the account name

Apple has built a robust set of services to help users get even more utility and productivity out of their devices, including iMessage, FaceTime, Siri, Spotlight Suggestions, iCloud, iCloud Backup, and iCloud Keychain.

These Internet services have been built with the same security goals that iOS promotes throughout the platform. These goals include secure handling of data, whether at rest on the device or in transit over wireless networks; protection of users' personal information; and threat protection against malicious or unauthorized access to information and services. Each service uses its own powerful security architecture without compromising the overall ease of use of iOS.

Apple ID

An Apple ID is the user name and password that is used to sign in to Apple services such as iCloud, iMessage, FaceTime, the iTunes Store, the iBooks Store, the App Store, and more. It is important for users to keep their Apple IDs secure to prevent unauthorized access to their accounts. To help with this, Apple requires strong passwords that must be at least eight characters in length, contain both letters and numbers, must not contain more than three consecutive identical characters, and cannot be a commonly used password. Users are encouraged to exceed these guidelines by adding extra characters and punctuation marks to make their passwords even stronger. Apple also sends email and push notifications to users when important changes are made to their account; for example, if a password or billing information has been changed, or the Apple ID has been used to sign in on a new device. If anything does not look familiar, users are instructed to change their Apple ID password immediately.

Apple also offers two-step verification for Apple ID, which provides a second layer of security for the user's account. With two-step verification enabled, the user's identity must be verified via a temporary code sent to one of the user's trusted devices before changes are permitted to his or her Apple ID account information, before signing in to iCloud, iMessage, FaceTime, and Game Center, and before making an iTunes Store, iBooks Store, or App Store purchase from a new device. This can prevent anyone from accessing a user's account, even if they know the password. Users are also provided with a 14-character Recovery Key to be stored in a safe place in case they ever forget their password or lose access to their trusted devices.

For more information on two-step verification for Apple ID, visit <https://support.apple.com/kb/ht5570>.

iMessage

Apple iMessage is a messaging service for iOS devices and Mac computers. iMessage supports text and attachments such as photos, contacts, and locations. Messages appear on all of a user's registered devices so that a conversation can be continued from any of the user's devices. iMessage makes extensive use of the Apple Push Notification service (APNs). Apple does not log messages or attachments, and their contents are protected by end-to-end encryption so no one but the sender and receiver can access them. Apple cannot decrypt the data.

When a user turns on iMessage on a device, the device generates two pairs of keys for use with the service: an RSA 1280-bit key for encryption and an ECDSA 256-bit key on the NIST P-256 curve for signing. The private keys for both key pairs are saved in the device's keychain and the public keys are sent to Apple's directory service (IDS), where they are associated with the user's phone number or email address, along with the device's APNs address.

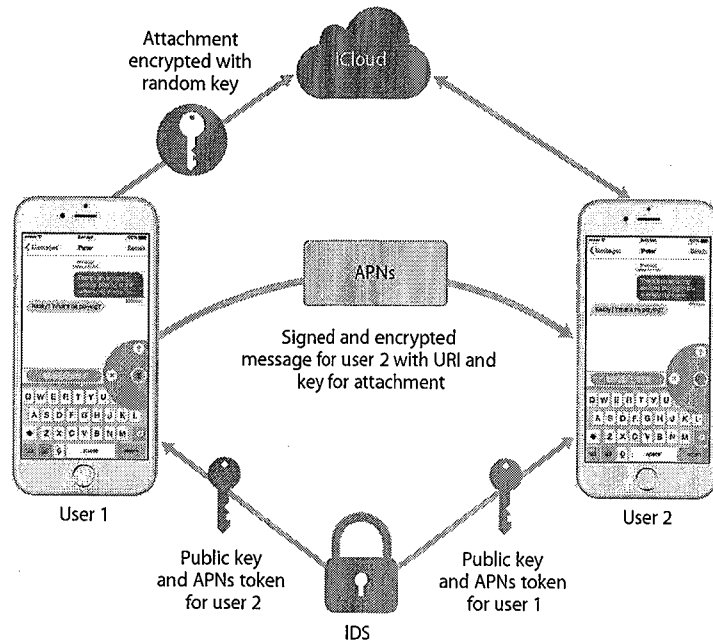
As users enable additional devices for use with iMessage, their encryption and signing public keys, APNs addresses, and associated phone numbers are added to the directory service. Users can also add more email addresses, which will be verified by sending a confirmation link. Phone numbers are verified by the carrier network and SIM. Further, all of the user's registered devices display an alert message when a new device, phone number, or email address is added.

How iMessage sends and receives messages

Users start a new iMessage conversation by entering an address or name. If they enter a phone number or email address, the device contacts the IDS to retrieve the public keys and APNs addresses for all of the devices associated with the addressee. If the user enters a name, the device first utilizes the user's Contacts app to gather the phone numbers and email addresses associated with that name, then gets the public keys and APNs addresses from the IDS.

The user's outgoing message is individually encrypted for each of the receiver's devices. The public RSA encryption keys of the receiving devices are retrieved from IDS. For each receiving device, the sending device generates a random 128-bit key and encrypts the message with it using AES in CTR mode. This per-message AES key is encrypted using RSA-OAEP to the public key of the receiving device. The combination of the encrypted message text and the encrypted message key is then hashed with SHA-1, and the hash is signed with ECDSA using the sending device's private signing key. The resulting messages, one for each receiving device, consist of the encrypted message text, the encrypted message key, and the sender's digital signature. They are then dispatched to the APNs for delivery. Metadata, such as the timestamp and APNs routing information, is not encrypted. Communication with APNs is encrypted using a forward-secret TLS channel.

APNs can only relay messages up to 4 KB or 16 KB in size, depending on iOS version. If the message text is too long, or if an attachment such as a photo is included, the attachment is encrypted using AES in CTR mode with a randomly generated 256-bit key and uploaded to iCloud. The AES key for the attachment, its URI (Uniform Resource Identifier), and a SHA-1 hash of its encrypted form are then sent to the recipient as the contents of an iMessage, with their confidentiality and integrity protected through normal iMessage encryption, as shown below.



For group conversations, this process is repeated for each recipient and their devices.

On the receiving side, each device receives its copy of the message from APNs, and, if necessary, retrieves the attachment from iCloud. The incoming phone number or email address of the sender is matched to the receiver's contacts so that a name can be displayed, if possible.

As with all push notifications, the message is deleted from APNs when it is delivered. Unlike other APNs notifications, however, iMessage messages are queued for delivery to offline devices. Messages are currently stored for up to 30 days.

FaceTime

FaceTime is Apple's video and audio calling service. Similar to iMessage, FaceTime calls also use the Apple Push Notification service to establish an initial connection to the user's registered devices. The audio/video contents of FaceTime calls are protected by end-to-end encryption, so no one but the sender and receiver can access them. Apple cannot decrypt the data.

FaceTime uses Internet Connectivity Establishment (ICE) to establish a peer-to-peer connection between devices. Using Session Initiation Protocol (SIP) messages, the devices verify their identity certificates and establish a shared secret for each session. The cryptographic nonces supplied by each device are combined to salt keys for each of the media channels, which are streamed via Secure Real Time Protocol (SRTP) using AES-256 encryption.

iCloud

iCloud stores a user’s contacts, calendars, photos, documents, and more and keeps the information up to date across all of his or her devices, automatically. iCloud can also be used by third-party apps to store and sync documents as well as key values for app data as defined by the developer. Users set up iCloud by signing in with an Apple ID and choosing which services they would like to use. iCloud features, including My Photo Stream, iCloud Drive, and Backup, can be disabled by IT administrators via a configuration profile. The service is agnostic about what is being stored and handles all file content the same way, as a collection of bytes.

Each file is broken into chunks and encrypted by iCloud using AES-128 and a key derived from each chunk’s contents that utilizes SHA-256. The keys, and the file’s metadata, are stored by Apple in the user’s iCloud account. The encrypted chunks of the file are stored, without any user-identifying information, using third-party storage services, such as Amazon S3 and Windows Azure.

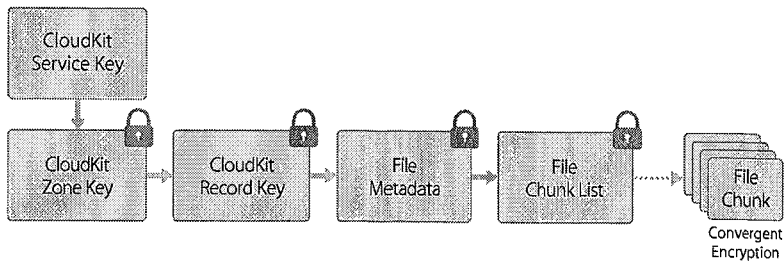
iCloud Drive

iCloud Drive adds account-based keys to protect documents stored in iCloud. As with existing iCloud services, it chunks and encrypts file contents and stores the encrypted chunks using third-party services. However, the file content keys are wrapped by record keys stored with the iCloud Drive metadata. These record keys are in turn protected by the user’s iCloud Drive service key, which is then stored with the user’s iCloud account. Users get access to their iCloud documents metadata by having authenticated with iCloud, but must also possess the iCloud Drive service key to expose protected parts of iCloud Drive storage.

CloudKit

CloudKit allows app developers to store key-value data, structured data, and assets in iCloud. Access to CloudKit is controlled using app entitlements. CloudKit supports both public and private databases. Public databases are used by all copies of the app, typically for general assets, and are not encrypted. Private databases store the user’s data.

As with iCloud Drive, CloudKit uses account-based keys to protect the information stored in the user’s private database and, similar to other iCloud services, files are chunked, encrypted, and stored using third-party services. CloudKit utilizes a hierarchy of keys, similar to Data Protection. The per-file keys are wrapped by CloudKit Record keys. The Record keys, in turn, are protected by a zone-wide key, which is protected by the user’s CloudKit Service key. The CloudKit Service key is stored in the user’s iCloud account and is available only after the user has authenticated with iCloud.



iCloud Backup

iCloud also backs up information—including device settings, app data, photos, and videos in the Camera Roll, and conversations in the Messages app—daily over Wi-Fi. iCloud secures the content by encrypting it when sent over the Internet, storing it in an encrypted format, and using secure tokens for authentication. iCloud Backup occurs only when the device is locked, connected to a power source, and has Wi-Fi access to the Internet. Because of the encryption used in iOS, the system is designed to keep data secure while allowing incremental, unattended backup and restoration to occur.

Here's what iCloud backs up:

- Information about purchased music, movies, TV shows, apps, and books, but not the purchased content itself
- Photos and videos in Camera Roll
- Contacts, calendar events, reminders, and notes
- Device settings
- App data
- PDFs and books added to iBooks but not purchased
- Call history
- Home screen and app organization
- iMessage, text (SMS), and MMS messages
- Ringtones
- HomeKit data
- HealthKit data
- Visual Voicemail

When files are created in Data Protection classes that are not accessible when the device is locked, their per-file keys are encrypted using the class keys from the iCloud Backup keybag. Files are backed up to iCloud in their original, encrypted state. Files in Data Protection class No Protection are encrypted during transport.

The iCloud Backup keybag contains asymmetric (Curve25519) keys for each Data Protection class, which are used to encrypt the per-file keys. For more information about the contents of the backup keybag and the iCloud Backup keybag, see "Keychain Data Protection" in the Encryption and Data Protection section.

The backup set is stored in the user's iCloud account and consists of a copy of the user's files, and the iCloud Backup keybag. The iCloud Backup keybag is protected by a random key, which is also stored with the backup set. (The user's iCloud password is not utilized for encryption so that changing the iCloud password won't invalidate existing backups.)

While the user's keychain database is backed up to iCloud, it remains protected by a UID-tangled key. This allows the keychain to be restored only to the same device from which it originated, and it means no one else, including Apple, can read the user's keychain items.

On restore, the backed-up files, iCloud Backup keybag, and the key for the keybag are retrieved from the user's iCloud account. The iCloud Backup keybag is decrypted using its key, then the per-file keys in the keybag are used to decrypt the files in the backup set, which are written as new files to the file system, thus re-encrypting them as per their Data Protection class.

Safari integration with iCloud Keychain

Safari can automatically generate cryptographically strong random strings for website passwords, which are stored in Keychain and synced to your other devices. Keychain items are transferred from device to device, traveling through Apple servers, but are encrypted in such a way that Apple and other devices cannot read their contents.

iCloud Keychain

iCloud Keychain allows users to securely sync his or her passwords between iOS devices and Mac computers without exposing that information to Apple. In addition to strong privacy and security, other goals that heavily influenced the design and architecture of iCloud Keychain were ease of use and the ability to recover a keychain. iCloud Keychain consists of two services: keychain syncing and keychain recovery.

Apple designed iCloud Keychain and keychain recovery so that a user's passwords are still protected under the following conditions:

- A user's iCloud account is compromised.
- iCloud is compromised by an external attacker or employee.
- Third-party access to user accounts.

Keychain syncing

When a user enables iCloud Keychain for the first time, the device establishes a circle of trust and creates a syncing identity for itself. A syncing identity consists of a private key and a public key. The public key of the syncing identity is put in the circle, and the circle is signed twice: first by the private key of the syncing identity, then again with an asymmetric elliptical key (using P256) derived from the user's iCloud account password. Also stored with the circle are the parameters (random salt and iterations) used to create the key that is based on the user's iCloud password.

The signed syncing circle is placed in the user's iCloud key value storage area. It cannot be read without knowing the user's iCloud password, and cannot be modified validly without having the private key of the syncing identity of its member.

When the user turns on iCloud Keychain on another device, the new device notices in iCloud that the user has a previously established syncing circle that it is not a member of. The device creates its syncing identity key pair, then creates an application ticket to request membership in the circle. The ticket consists of the device's public key of its syncing identity, and the user is asked to authenticate with his or her iCloud password. The elliptical key generation parameters are retrieved from iCloud and generate a key that is used to sign the application ticket. Finally, the application ticket is placed in iCloud.

When the first device sees that an application ticket has arrived, it displays a notice for the user to acknowledge that a new device is asking to join the syncing circle. The user enters his or her iCloud password, and the application ticket is verified as signed by a matching private key. This establishes that the person who generated the request to join the circle entered the user's iCloud password at the time the request was made.

Upon the user's approval to add the new device to the circle, the first device adds the public key of the new member to the syncing circle, signs it again with both its syncing identity and the key derived from the user's iCloud password. The new syncing circle is placed in iCloud, where it is similarly signed by the new member of the circle.

There are now two members of the signing circle, and each member has the public key of its peer. They now begin to exchange individual keychain items via iCloud key value storage. If both circle members have the same item, the one with the most recent modification date will be synced. Items are skipped if the other member has the item and the modification dates are identical. Each item that is synced is encrypted specifically for the device it is being sent to. It cannot be decrypted by other devices or Apple. Additionally, the encrypted item is ephemeral in iCloud; it's overwritten with each new item that's synced.

This process is repeated as new devices join the syncing circle. For example, when a third device joins, the confirmation appears on both of the other user's devices. The user can approve the new member from either of those devices. As new peers are added, each peer syncs with the new one to ensure that all members have the same keychain items.

However, the entire keychain is not synced. Some items are device-specific, such as VPN identities, and shouldn't leave the device. Only items with the attribute `kSecAttrSynchronizable` are synced. Apple has set this attribute for Safari user data (including user names, passwords, and credit card numbers), as well as Wi-Fi passwords and HomeKit encryption keys.

Additionally, by default, keychain items added by third-party apps do not sync. Developers must set the `kSecAttrSynchronizable` when adding items to the keychain.

Keychain recovery

Keychain recovery provides a way for users to optionally escrow their keychain with Apple, without allowing Apple to read the passwords and other data it contains. Even if the user has only a single device, keychain recovery provides a safety net against data loss. This is particularly important when Safari is used to generate random, strong passwords for web accounts, as the only record of those passwords is in the keychain.

A cornerstone of keychain recovery is secondary authentication and a secure escrow service, created by Apple specifically to support this feature. The user's keychain is encrypted using a strong passcode, and the escrow service will provide a copy of the keychain only if a strict set of conditions are met.

When iCloud Keychain is turned on, the user is asked to create an iCloud Security Code. This code is required to recover an escrowed keychain. By default, the user is asked to provide a simple four-digit value for the security code. However, users can also specify their own, longer code, or let their devices create a cryptographically random code that they can record and keep on their own.

Next, the iOS device exports a copy of the user's keychain, encrypts it wrapped with keys in an asymmetric keybag, and places it in the user's iCloud key value storage area. The keybag is wrapped with the user's iCloud Security Code and the public key of the HSM (hardware security module) cluster that will store the escrow record. This becomes the user's iCloud Escrow Record.

If the user decided to accept a cryptographically random security code, instead of specifying his or her own or using a four-digit value, no escrow record is necessary. Instead, the iCloud Security Code is used to wrap the random key directly.

In addition to establishing a security code, users must register a phone number. This is used to provide a secondary level of authentication during keychain recovery. The user will receive an SMS that must be replied to in order for the recovery to proceed.

Escrow security

iCloud provides a secure infrastructure for keychain escrow that ensures only authorized users and devices can perform a recovery. Topographically positioned behind iCloud are clusters of hardware security modules (HSM). These clusters guard the escrow records. Each has a key that is used to encrypt the escrow records under their watch, as described previously.

To recover a keychain, users must authenticate with their iCloud account and password and respond to an SMS sent to their registered phone number. Once this is done, users must enter their iCloud Security Code. The HSM cluster verifies that a user knows his or her iCloud Security Code using Secure Remote Password protocol (SRP); the code itself is not sent to Apple. Each member of the cluster independently verifies that the user has not exceeded the maximum number of attempts that are allowed to retrieve his or her record, as discussed below. If a majority agree, the cluster unwraps the escrow record and sends it to the user's device.

Next, the device uses the iCloud Security Code to unwrap the random key used to encrypt the user's keychain. With that key, the keychain—retrieved from iCloud key value storage—is decrypted and restored onto the device. Only 10 attempts to authenticate and retrieve an escrow record are allowed. After several failed attempts, the record is locked and the user must call Apple Support to be granted more attempts. After the 10th failed attempt, the HSM cluster destroys the escrow record and the keychain is lost forever. This provides protection against a brute-force attempt to retrieve the record, at the expense of sacrificing the keychain data in response.

These policies are coded in the HSM firmware. The administrative access cards that permit the firmware to be changed have been destroyed. Any attempt to alter the firmware or access the private key will cause the HSM cluster to delete the private key. Should this occur, the owners of all keychains protected by the cluster will receive a message informing them that their escrow record has been lost. They can then choose to re-enroll.

Siri

By simply talking naturally, users can enlist Siri to send messages, schedule meetings, place phone calls, and more. Siri uses speech recognition, text-to-speech, and a client-server model to respond to a broad range of requests. The tasks that Siri supports have been designed to ensure that only the absolute minimal amount of personal information is utilized and that it is fully protected.

When Siri is turned on, the device creates random identifiers for use with the voice recognition and Siri servers. These identifiers are used only within Siri and are utilized to improve the service. If Siri is subsequently turned off, the device will generate a new random identifier to be used if Siri is turned back on.

In order to facilitate Siri's features, some of the user's information from the device is sent to the server. This includes information about the music library (song titles, artists, and playlists), the names of Reminders lists, and names and relationships that are defined in Contacts. All communication with the server is over HTTPS.

When a Siri session is initiated, the user's first and last name (from Contacts), along with a rough geographic location, is sent to the server. This is so Siri can respond with the name or answer questions that only need an approximate location, such as those about the weather.

If a more precise location is necessary, for example, to determine the location of nearby movie theaters, the server asks the device to provide a more exact location. This is an example of how, by default, information is sent to the server only when it's strictly necessary to process the user's request. In any event, session information is discarded after 10 minutes of inactivity.

When Siri is used from Apple Watch, the watch creates its own random unique identifier, as described above. However, instead of sending the user's information again, its requests also send the Siri identifier of the paired iPhone to provide a reference to that information.

The recording of the user's spoken words is sent to Apple's voice recognition server. If the task involves dictation only, the recognized text is sent back to the device. Otherwise, Siri analyzes the text and, if necessary, combines it with information from the profile associated with the device. For example, if the request is "send a message to my mom," the relationships and names that were uploaded from Contacts are utilized. The command for the identified action is then sent back to the device to be carried out.

Many Siri functions are accomplished by the device under the direction of the server. For example, if the user asks Siri to read an incoming message, the server simply tells the device to speak the contents of its unread messages. The contents and sender of the message are not sent to the server.

User voice recordings are saved for a six-month period so that the recognition system can utilize them to better understand the user's voice. After six months, another copy is saved, without its identifier, for use by Apple in improving and developing Siri for up to two years. Additionally, some recordings that reference music, sports teams and players, and businesses or points of interest are similarly saved for purposes of improving Siri.

Siri can also be invoked hands-free via voice activation. The voice trigger detection is performed locally on the device. In this mode, Siri is activated only when the incoming audio pattern sufficiently matches the acoustics of the specified trigger phrase. When the trigger is detected, the corresponding audio including the subsequent Siri command is sent to Apple's voice recognition server for further processing, which follows the same rules as other user voice recordings made through Siri.

Continuity

Continuity takes advantage of technologies like iCloud, Bluetooth, and Wi-Fi to enable users to continue an activity from one device to another, make and receive phone calls, send and receive text messages, and share a cellular Internet connection.

Handoff

With Handoff, when a user's Mac and iOS device are near each other, the user can automatically pass whatever they're working on from one device to the other. Handoff lets the user switch devices and instantly continue working.

When a user signs in to iCloud on a second Handoff capable device, the two devices establish a Bluetooth Low Energy 4.0 pairing out-of-band using the Apple Push Notification service (APNs). The individual messages are encrypted in a similar fashion to iMessage. Once the devices are paired, each will generate a symmetric 256-bit AES key that gets stored in the device's keychain. This key is used to encrypt and authenticate the Bluetooth Low Energy advertisements that communicate the device's current activity to other iCloud paired devices using AES-256 in GCM mode, with replay protection measures. The first time a device receives an advertisement from a new key, it will establish a Bluetooth Low Energy connection to the originating device and perform an advertisement encryption key exchange. This connection is secured using standard Bluetooth Low Energy 4.0 encryption as well as encryption of the individual messages, which is similar to how iMessage is encrypted. In some situations, these messages will go via the Apple Push Notification service instead of Bluetooth Low Energy. The activity payload is protected and transferred in the same way as an iMessage.

Handoff between native apps and websites

Handoff allows an iOS native app to resume webpages in domains legitimately controlled by the app developer. It also allows the native app user activity to be resumed in a web browser.

To prevent native apps from claiming to resume websites not controlled by the developer, the app must demonstrate legitimate control over the web domains it wants to resume. Control over a website domain is established via the mechanism used for shared web credentials. For details, refer to "Access to Safari saved passwords" in the Encryption and Data Protection section. The system must validate an app's domain name control before the app is permitted to accept user activity Handoff.

The source of a webpage Handoff can be any browser that has adopted the Handoff APIs. When the user views a webpage, the system advertises the domain name of the webpage in the encrypted Handoff advertisement bytes. Only the user's other devices can decrypt the advertisement bytes (as previously described in the section above).

On a receiving device, the system detects that an installed native app accepts Handoff from the advertised domain name and displays that native app icon as the Handoff option. When launched, the native app receives the full URL and the title of the webpage. No other information is passed from the browser to the native app.

In the opposite direction, a native app may specify a fallback URL when a Handoff-receiving device does not have the same native app installed. In this case, the system displays the user's default browser as the Handoff app option (if that browser has adopted Handoff APIs). When Handoff is requested, the browser will be launched and given the fallback URL provided by the source app. There is no requirement that the fallback URL be limited to domain names controlled by the native app developer.

Handoff of larger data

In addition to the basic feature of Handoff, some apps may elect to use APIs that support sending larger amounts of data over Apple-created peer-to-peer Wi-Fi technology (in a similar fashion to AirDrop). For example, the Mail app uses these APIs to support Handoff of a mail draft, which may include large attachments.

When an app uses this facility, the exchange between the two devices starts off just as in Handoff (see previous sections). However, after receiving the initial payload using Bluetooth Low Energy, the receiving device initiates a new connection over Wi-Fi. This connection is encrypted (TLS), which exchanges their iCloud identity certificates. The identity in the certificates is verified against the user's identity. Further payload data is sent over this encrypted connection until the transfer is complete.

iPhone Cellular Call Relay

When your Mac, iPad, or iPod is on the same Wi-Fi network as your iPhone, it can make and receive phone calls using your iPhone cellular connection. Configuration requires your devices to be signed in to both iCloud and FaceTime using the same Apple ID account.

When an incoming call arrives, all configured devices will be notified via the Apple Push Notification service (APNs), with each notification using the same end-to-end encryption as iMessage uses. Devices that are on the same network will present the incoming call notification UI. Upon answering the call, the audio will be seamlessly transmitted from your iPhone using a secure peer-to-peer connection between the two devices.

Outgoing calls will also be relayed to iPhone via the Apple Push Notification service, and audio will be similarly transmitted over the secure peer-to-peer link between devices.

Users can disable phone call relay on a device by turning off iPhone Cellular Calls in FaceTime settings.

iPhone Text Message Forwarding

Text Message Forwarding automatically sends SMS text messages received on iPhone to a user's enrolled iPad, iPod touch, or Mac. Each device must be signed in to the iMessage service using the same Apple ID account. When SMS Message Forwarding is turned on, enrollment is verified on each device by entering a random six-digit numeric code generated by iPhone.

Once devices are linked, iPhone encrypts and forwards incoming SMS text messages to each device, utilizing the methods described in the iMessage section of this document. Replies are sent back to iPhone using the same method, then iPhone sends the reply as a text message using the carrier's SMS transmission mechanism. Text Message Forwarding can be turned on or off in Messages settings.

Instant Hotspot

iOS devices that support Instant Hotspot use Bluetooth Low Energy to discover and communicate to devices that have signed in to the same iCloud account. Compatible Mac computers running OS X Yosemite and later use the same technology to discover and communicate with Instant Hotspot iOS devices.

When a user enters Wi-Fi Settings on the iOS device, the device emits a Bluetooth Low Energy signal containing an identifier that all devices signed in to the same iCloud account agree upon. The identifier is generated from a DSID (Destination Signaling Identifier) tied to the iCloud account, and rotated periodically. When other devices signed in to the same iCloud account are in close proximity and support personal hotspot, they detect the signal and respond, indicating availability.

When a user chooses a device available for personal hotspot, a request to turn on Personal Hotspot is sent to that device. The request is sent across a link that is encrypted using standard Bluetooth Low Energy encryption, and the request is encrypted in a fashion similar to iMessage encryption. The device then responds across the same Bluetooth Low Energy link using the same per-message encryption with personal hotspot connection information.

Spotlight Suggestions

Safari search and Spotlight search include search suggestions from the Internet, apps, iTunes, App Store, movie showtimes, locations nearby, and more.

To make suggestions more relevant to users, user context and search feedback with search query requests are sent to Apple. Context sent with search requests provides Apple with: i) the device's approximate location; ii) the device type (e.g., Mac, iPhone, iPad, or iPod); iii) the client app, which is either Spotlight or Safari; iv) the device's default language and region settings; v) the three most recently used apps on the device; and vi) an anonymous session ID. All communication with the server is encrypted via HTTPS.

To help protect user privacy, Spotlight Suggestions never sends exact location, instead blurring the location on the client before sending. The level of blurring is based on estimated population density at the device's location; for instance, more blurring is used in a rural location versus less blurring in a city center where users will typically be closer together. Further, users can disable the sending of all location information to Apple in Settings, by turning off Location Services for Spotlight Suggestions. If Location Services is disabled, then Apple may use the client's IP address to infer an approximate location.

The anonymous session ID allows Apple to analyze patterns between queries conducted in a 15-minute period. For instance, if users frequently search for "Café phone number" shortly after searching for "Café," Apple may learn to make the phone number more available in results. Unlike most search engines, however, Apple's search service does not use a persistent personal identifier across a user's search history to tie queries to a user or device; instead, Apple devices use a temporary anonymous session ID for at most a 15-minute period before discarding that ID.

Information on the three most recently used apps on the device is included as additional search context. To protect the privacy of users, only apps that are in an Apple-maintained whitelist of popular apps and have been accessed within the last three hours are included.

Search feedback sent to Apple provides Apple with: i) timings between user actions such as key-presses and result selections; ii) Spotlight Suggestions result selected, if any; and iii) type of local result selected (e.g., "Bookmark" or "Contact"). Just as with search context, the search feedback is not tied to any individual person or device.

Apple retains Spotlight Suggestions logs with queries, context, and feedback for up to 18 months. Reduced logs including only query, country, language, date (to the hour), and device-type are retained up to two years. IP addresses are not retained with query logs.

In some cases, Spotlight Suggestions may forward queries for common words and phrases to a qualified partner in order to receive and display the partner's search results. These queries are not stored by the qualified partner and partners do not receive search feedback. Partners also do not receive user IP addresses. Communication with the partner is encrypted via HTTPS. Apple will provide city-level location, device type, and client language as search context to the partner based on which locations, device types, and languages Apple sees repeated queries from.

Spotlight Suggestions can be turned off in Settings for Spotlight, for Safari, or for both. If turned off for Spotlight, then Spotlight is reverted to being a local on-device-only search client that does not transmit information to Apple. If turned off in Safari, the user's search queries, search context, and search feedback are not transmitted to Apple.

Spotlight also includes mechanisms for making local, on-device content searchable:

- The CoreSpotlight API, which allows Apple and third-party apps to pass indexable content to Spotlight.
- The NSUserActivity API, which allows Apple and third-party apps to pass information to Spotlight regarding app pages visited by the user.

Spotlight maintains an on-device index of the information it receives using these two methods, so that results from this data can be shown in response to a user's search, or automatically when Spotlight is launched. There is also an on-device federated search API, only available to Apple-provided apps, which allows Spotlight to pass user search queries to apps for processing, and receive their results.

Device Controls

iOS supports flexible security policies and configurations that are easy to enforce and manage. This enables organizations to protect corporate information and ensure that employees meet enterprise requirements, even if they are using devices they've provided themselves—for example, as part of a "bring your own device" (BYOD) program.

Organizations can use resources such as passcode protection, configuration profiles, remote wipe, and third-party MDM solutions to manage fleets of devices and help keep corporate data secure, even when employees access this data on their personal iOS devices.

Passcode protection

By default, the user's passcode can be defined as a numeric PIN. On devices with Touch ID, the minimum passcode length is six digits. On other devices, the minimum length is four digits. Users can specify a longer alphanumeric passcode by selecting Custom Alphanumeric Code in the Passcode Options in Settings > Passcode. Longer and more complex passcodes are harder to guess or attack, and are recommended for enterprise use.

Administrators can enforce complex passcode requirements and other policies using MDM or Exchange ActiveSync, or by requiring users to manually install configuration profiles. The following passcode policies are available:

- Allow simple value
- Require alphanumeric value
- Minimum passcode length
- Minimum number of complex characters
- Maximum passcode age
- Passcode history
- Auto-lock timeout
- Grace period for device lock
- Maximum number of failed attempts
- Allow Touch ID

For details about each policy, see the Configuration Profile Key Reference documentation at <https://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/>.

iOS pairing model

iOS uses a pairing model to control access to a device from a host computer. Pairing establishes a trust relationship between the device and its connected host, signified by public key exchange. iOS uses this sign of trust to enable additional functionality with the connected host, such as data synchronization. In iOS 9, services that require pairing cannot be started until after the device has been unlocked by the user.

The pairing process requires the user to unlock the device and accept the pairing request from the host. After the user has done this, the host and device exchange and save 2048-bit RSA public keys. The host is then given a 256-bit key that can unlock an escrow keybag stored on the device (see Escrow keybags in the Keybags section). The exchanged keys are used to start an encrypted SSL session, which the device requires before it will send protected data to the host or start a service (iTunes syncing, file transfers, Xcode development, etc.). The device requires connections from a host over Wi-Fi to use this encrypted session for all communication, so it must have been previously paired over USB. Pairing also enables several diagnostic capabilities. In iOS 9, if a pairing record has not been used for more than six months, it expires. For more information, see <https://support.apple.com/kb/HT6331>.

Certain services, including `com.apple.pcapd`, are restricted to work only over USB. Additionally, the `com.apple.file_relay` service requires an Apple-signed configuration profile to be installed.

A user can clear the list of trusted hosts by using the “Reset Network Settings” or “Reset Location & Privacy” options. For more information, see <https://support.apple.com/kb/HT5868>.

Configuration enforcement

A configuration profile is an XML file that allows an administrator to distribute configuration information to iOS devices. Settings that are defined by an installed configuration profile can't be changed by the user. If the user deletes a configuration profile, all the settings defined by the profile are also removed. In this manner, administrators can enforce settings by tying policies to access. For example, a configuration profile that provides an email configuration can also specify a device passcode policy. Users won't be able to access mail unless their passcodes meet the administrator's requirements.

An iOS configuration profile contains a number of settings that can be specified, including:

- Passcode policies
- Restrictions on device features (disabling the camera, for example)
- Wi-Fi settings
- VPN settings
- Mail server settings
- Exchange settings
- LDAP directory service settings
- CalDAV calendar service settings
- Web clips
- Credentials and keys
- Advanced cellular network settings

Configuration profiles can be signed and encrypted to validate their origin, ensure their integrity, and protect their contents. Configuration profiles are encrypted using CMS (RFC 3852), supporting 3DES and AES-128.

Configuration profiles can also be locked to a device to completely prevent their removal, or to allow removal only with a passcode. Since many enterprise users own their iOS devices, configuration profiles that bind a device to an MDM server can be removed—but doing so will also remove all managed configuration information, data, and apps.

Users can install configuration profiles directly on their devices using Apple Configurator, or they can be downloaded via Safari, sent via a mail message, or sent over the air using an MDM server.

Mobile device management (MDM)

iOS support for MDM allows businesses to securely configure and manage scaled iPhone and iPad deployments across their organizations. MDM capabilities are built on existing iOS technologies such as configuration profiles, over-the-air enrollment, and the Apple Push Notification service (APNs). For example, APNs is used to wake the device so it can communicate directly with its MDM server over a secured connection. No confidential or proprietary information is transmitted via APNs.

Using MDM, IT departments can enroll iOS devices in an enterprise environment, wirelessly configure and update settings, monitor compliance with corporate policies, and even remotely wipe or lock managed devices. For more information on mobile device management, see www.apple.com/iphone/business/it/management.html.

Device Enrollment Program

The Device Enrollment Program (DEP) provides a fast, streamlined way to deploy iOS devices that an organization has purchased directly from Apple or through participating Apple Authorized Resellers and carriers. The organization can automatically enroll devices in MDM without having to physically touch or prep the devices before users get them. The setup process for users can be further simplified by removing specific steps in the Setup Assistant, so users are up and running quickly. Administrators can also control whether or not the user can remove the MDM profile from the device and ensure that device restrictions are in place from the very start. For example, they can order the devices from Apple, configure all the management settings, and have the devices shipped directly to the user's home address. Once the device is unboxed and activated, the device enrolls in the organization's MDM—and all management settings, apps, and books are ready for the user.

The process is simple: After enrolling in the program, administrators log in to the program website, link the program to their MDM server, and "claim" the iOS devices purchased through Apple. The devices can then be assigned to users via MDM. Once a user has been assigned, any MDM-specified configurations, restrictions, or controls are automatically installed. For more information, see <https://deploy.apple.com>.

Note: The Device Enrollment Program is not available in all countries or regions.

Apple Configurator

In addition to MDM, Apple Configurator for OS X makes it easy for anyone to deploy iOS devices. Apple Configurator can be used to quickly configure large numbers of devices with apps, data, restrictions, and settings.

Supervision

During the setup of a device, an organization can configure a device to be supervised. Supervision denotes that a device is institutionally owned, which provides additional control over its configuration and restrictions. Devices can be supervised during setup through the Device Enrollment Program or Apple Configurator.

For more information on configuring and managing devices using MDM or Apple Configurator, see the iOS Deployment Reference at <https://help.apple.com/deployment/ios>.

For information about the additional controls for supervised devices, see the Configuration Profile Reference: <https://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/iPhoneConfigurationProfileRef.pdf>.

Device restrictions

Administrators can restrict device features by installing a configuration profile. Some of the restrictions available include:

- Allow app installs
- Allow trusting enterprise apps
- Allow use of camera
- Allow FaceTime
- Allow screenshots
- Allow voice dialing while locked
- Allow automatic sync while roaming
- Allow in-app purchases
- Allow syncing of recent Mail
- Force user to enter store password for all purchases
- Allow Siri while device is locked
- Allow use of iTunes Store
- Allow documents from managed sources in unmanaged destinations
- Allow documents from unmanaged sources in managed destinations
- Allow iCloud Keychain sync
- Allow updating certificate trust database over the air
- Allow showing notifications on Lock screen
- Force AirPlay connections to use pairing passwords
- Allow Spotlight to show user-generated content from the Internet
- Enable Spotlight Suggestions in Spotlight
- Allow Handoff
- Treat AirDrop as unmanaged destination
- Allow enterprise books to be backed up
- Allow notes and bookmarks in enterprise books to sync across the user's devices
- Allow use of Safari

- Enable Safari autofill
- Force Fraudulent Website Warning
- Enable JavaScript
- Limit ad tracking in Safari
- Block pop-ups
- Accept cookies
- Allow iCloud backup
- Allow iCloud document and key-value sync
- Allow iCloud Photo Sharing
- Allow diagnostics to be sent to Apple
- Allow user to accept untrusted TLS certificates
- Force encrypted backups
- Allow Touch ID
- Allow Control Center access from Lock screen
- Allow Today view from Lock screen
- Require Apple Watch wrist detection

Supervised-only restrictions

- Allow iMessage
- Allow removal of apps
- Allow manual install of configuration profiles
- Global network proxy for HTTP
- Allow pairing to computers for content sync
- Restrict AirPlay connections with whitelist and optional connection passcodes
- Allow AirDrop
- Allow Find My Friends modification
- Allow autonomous Single App Mode for certain managed apps
- Allow account modification
- Allow cellular data modification
- Allow host pairing (iTunes)
- Allow Activation Lock
- Prevent Erase All Content and Settings
- Prevent enabling restrictions
- Third-party content filter
- Single App mode
- Always-on VPN
- Allow passcode modification
- Allow Apple Watch pairing
- Allow automatic app downloads
- Allow keyboard prediction, autocorrection, spell check, and short cuts

For more information about restrictions, see <https://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/iPhoneConfigurationProfileRef.pdf>

Remote wipe

iOS devices can be erased remotely by an administrator or user. Instant remote wipe is achieved by securely discarding the block storage encryption key from Effaceable Storage, rendering all data unreadable. A remote wipe command can be initiated by MDM, Exchange, or iCloud.

When a remote wipe command is triggered by MDM or iCloud, the device sends an acknowledgment and performs the wipe. For remote wipe via Exchange, the device checks in with the Exchange Server before performing the wipe.

Users can also wipe devices in their possession using the Settings app. And as mentioned, devices can be set to automatically wipe after a series of failed passcode attempts.

Find My iPhone and Activation Lock

If a device is lost or stolen, it's important to deactivate and erase the device. With iOS 7 or later, when Find My iPhone is turned on, the device can't be reactivated without entering the owner's Apple ID credentials. It's a good idea for an organization to either supervise its devices or have a policy in place for users to disable the feature so that Find My iPhone doesn't prevent the organization from assigning the device to another individual.

With iOS 7.1 or later, a compatible MDM solution can enable Activation Lock on supervised devices when a user turns on Find My iPhone. MDM administrators can manage Find My iPhone Activation Lock by supervising devices with Apple Configurator or the Device Enrollment Program. The MDM solution can then store a bypass code when Activation Lock is enabled, and later use this code to clear Activation Lock automatically when the device needs to be erased and assigned to a new user. See your MDM solution documentation for details.

Important: By default, supervised devices never have Activation Lock enabled, even if the user turns on Find My iPhone. However, an MDM server may retrieve a bypass code and permit Activation Lock on the device. If Find My iPhone is turned on when the MDM server enables Activation Lock, it is enabled at that point. If Find My iPhone is turned off when the MDM server enables Activation Lock, it's enabled the next time the user activates Find My iPhone.

Privacy Controls

Apple takes customer privacy seriously and has numerous built-in controls and options that allow iOS users to decide how and when apps utilize their information, as well as what information is being utilized.

Location Services

Location Services uses GPS, Bluetooth, and crowd-sourced Wi-Fi hotspot and cell tower locations to determine the user's approximate location. Location Services can be turned off using a single switch in Settings, or users can approve access for each app that uses the service. Apps may request to receive location data only while the app is being used or allow it at any time. Users may choose not to allow this access, and may change their choice at any time in Settings. From Settings, access can be set to never allowed, allowed when in use, or always, depending on the app's requested location use. Also, if apps granted access to use location at any time make use of this permission while in background mode, users are reminded of their approval and may change an app's access.

Additionally, users are given fine-grained control over system services' use of location information. This includes being able to turn off the inclusion of location information in information collected by the diagnostic and usage services used by Apple to improve iOS, location-based Siri information, location-based context for Spotlight Suggestions searches, local traffic conditions, and frequently visited locations used to estimate travel times.

Access to personal data

iOS helps prevent apps from accessing a user's personal information without permission. Additionally, in Settings, users can see which apps they have permitted to access certain information, as well as grant or revoke any future access. This includes access to:

- Contacts
- Calendars
- Reminders
- Photos
- Motion activity on iPhone 5s or later
- Social media accounts, such as Twitter and Facebook
- Microphone
- Camera
- HomeKit
- HealthKit
- Bluetooth sharing

If the user signs in to iCloud, apps are granted access by default to iCloud Drive. Users may control each app's access under iCloud in Settings. Additionally, iOS provides restrictions that prevent data movement between apps and accounts installed by MDM and those installed by the user.

Privacy policy

Apple's privacy policy is available online at <https://www.apple.com/legal/privacy>.

Conclusion

A commitment to security

Apple is committed to helping protect customers with leading privacy and security technologies that are designed to safeguard personal information, as well as comprehensive methods to help protect corporate data in an enterprise environment.

Security is built into iOS. From the platform to the network to the apps, everything a business needs is available in the iOS platform. Together, these components give iOS its industry-leading security without compromising the user experience.

Apple uses a consistent, integrated security infrastructure throughout iOS and the iOS apps ecosystem. Hardware-based storage encryption provides remote wipe capabilities when a device is lost, and enables users to completely remove all corporate and personal information when a device is sold or transferred to another owner. Diagnostic information is also collected anonymously.

iOS apps designed by Apple are built with enhanced security in mind. Safari offers safe browsing with support for Online Certificate Status Protocol (OCSP), EV certificates, and certificate verification warnings. Mail leverages certificates for authenticated and encrypted Mail by supporting S/MIME, which permits per-message S/MIME, so S/MIME users can choose to always sign and encrypt by default, or selectively control how individual messages are protected. iMessage and FaceTime also provide client-to-client encryption.

For third-party apps, the combination of required code signing, sandboxing, and entitlements gives users solid protection against viruses, malware, and other exploits that compromise the security of other platforms. The App Store submission process works to further shield users from these risks by reviewing every iOS app before it's made available for sale.

To make the most of the extensive security features built into iOS, businesses are encouraged to review their IT and security policies to ensure that they are taking full advantage of the layers of security technology offered by this platform.

Apple maintains a dedicated security team to support all Apple products. The team provides security auditing and testing for products under development, as well as for released products. The Apple team also provides security tools and training, and actively monitors for reports of new security issues and threats. Apple is a member of the Forum of Incident Response and Security Teams (FIRST). To learn more about reporting issues to Apple and subscribing to security notifications, go to apple.com/support/security.

Glossary

Address space layout randomization (ASLR)	A technique employed by iOS to make the successful exploitation of a software bug much more difficult. By ensuring memory addresses and offsets are unpredictable, exploit code can't hard code these values. In iOS 5 and later, the position of all system apps and libraries are randomized, along with all third-party apps compiled as position-independent executables.
Apple Push Notification service (APNs)	A worldwide service provided by Apple that delivers push notifications to iOS devices.
Boot ROM	The very first code executed by a device's processor when it first boots. As an integral part of the processor, it can't be altered by either Apple or an attacker.
Data Protection	File and keychain protection mechanism for iOS. It can also refer to the APIs that apps use to protect files and keychain items.
Device Firmware Upgrade (DFU)	A mode in which a device's Boot ROM code waits to be recovered over USB. The screen is black when in DFU mode, but upon connecting to a computer running iTunes, the following prompt is presented: "iTunes has detected an iPad in recovery mode. You must restore this iPad before it can be used with iTunes."
ECID	A 64-bit identifier that's unique to the processor in each iOS device. Used as part of the personalization process, it's not considered a secret.
Effaceable Storage	A dedicated area of NAND storage, used to store cryptographic keys, that can be addressed directly and wiped securely. While it doesn't provide protection if an attacker has physical possession of a device, keys held in Effaceable Storage can be used as part of a key hierarchy to facilitate fast wipe and forward security.
File system key	The key that encrypts each file's metadata, including its class key. This is kept in Effaceable Storage to facilitate fast wipe, rather than confidentiality.
Group ID (GID)	Like the UID but common to every processor in a class.
Hardware security module (HSM)	A specialized tamper-resistant computer that safeguards and manages digital keys.
iBoot	Code that's loaded by LLB, and in turn loads XNU, as part of the secure boot chain.
Identity Service (IDS)	Apple's directory of iMessage public keys, APNs addresses, and phone numbers and email addresses that are used to look up the keys and device addresses.
Integrated circuit (IC)	Also known as a microchip.
Joint Test Action Group (JTAG)	Standard hardware debugging tool used by programmers and circuit developers.
Keybag	<p>A data structure used to store a collection of class keys. Each type (system, backup, escrow, or iCloud Backup) has the same format:</p> <ul style="list-style-type: none"> • A header containing: <ul style="list-style-type: none"> – Version (set to 3 in iOS 5) – Type (system, backup, escrow, or iCloud Backup) – Keybag UUID – An HMAC if the keybag is signed – The method used for wrapping the class keys: tangling with the UID or PBKDF2, along with the salt and iteration count • A list of class keys: <ul style="list-style-type: none"> – Key UUID – Class (which file or keychain Data Protection class this is) – Wrapping type (UID-derived key only; UID-derived key and passcode-derived key) – Wrapped class key – Public key for asymmetric classes

Keychain	The infrastructure and a set of APIs used by iOS and third-party apps to store and retrieve passwords, keys, and other sensitive credentials.
Key wrapping	Encrypting one key with another. iOS uses NIST AES key wrapping, as per RFC 3394.
Low-Level Bootloader (LLB)	Code that's invoked by the Boot ROM, and in turn loads iBoot, as part of the secure boot chain.
Per-file key	The AES 256-bit key used to encrypt a file on the file system. The per-file key is wrapped by a class key and is stored in the file's metadata.
Provisioning Profile	A plist signed by Apple that contains a set of entities and entitlements allowing apps to be installed and tested on an iOS device. A development Provisioning Profile lists the devices that a developer has chosen for ad hoc distribution, and a distribution Provisioning Profile contains the app ID of an enterprise-developed app.
Ridge flow angle mapping	A mathematical representation of the direction and width of the ridges extracted from a portion of a fingerprint.
Smart card	An integrated, embedded circuit that provides secure identification, authentication, and data storage.
System on a chip (SoC)	An integrated circuit (IC) that incorporates multiple components into a single chip. The Secure Enclave is an SoC within Apple's A7-or-later central processor.
Tangling	The process by which a user's passcode is turned into a cryptographic key and strengthened with the device's UID. This ensures that a brute-force attack must be performed on a given device, and thus is rate limited and cannot be performed in parallel. The tangling algorithm is PBKDF2, which uses AES keyed with the device UID as the pseudorandom function (PRF) for each iteration.
Uniform Resource Identifier (URI)	A string of characters that identifies a web-based resource.
Unique ID (UID)	A 256-bit AES key that's burned into each processor at manufacture. It cannot be read by firmware or software, and is used only by the processor's hardware AES engine. To obtain the actual key, an attacker would have to mount a highly sophisticated and expensive physical attack against the processor's silicon. The UID is not related to any other identifier on the device including, but not limited to, the UDID.
XNU	The kernel at the heart of the iOS and OS X operating systems. It's assumed to be trusted, and enforces security measures such as code signing, sandboxing, entitlement checking, and ASLR.

Document Revision History

Date	Summary
September 2015	<p data-bbox="841 453 993 483">Updated for iOS 9</p> <ul style="list-style-type: none"> <li data-bbox="841 491 1078 520">• Apple Watch activation lock <li data-bbox="841 529 993 558">• Passcode policies <li data-bbox="841 567 1026 596">• Touch ID API support <li data-bbox="841 604 1143 634">• Data Protection on A8 uses AES-XTS <li data-bbox="841 642 1182 672">• Keybags for unattended software update <li data-bbox="841 680 1019 709">• Certification updates <li data-bbox="841 718 1068 747">• Enterprise app trust model <li data-bbox="841 756 1149 785">• Data protection for Safari bookmarks <li data-bbox="841 793 1036 823">• App Transport Security <li data-bbox="841 831 1000 861">• VPN specifications <li data-bbox="841 869 1133 898">• iCloud Remote Access for HomeKit <li data-bbox="841 907 1052 936">• Apple Pay Rewards cards <li data-bbox="841 945 1068 974">• Apple Pay card issuer's app <li data-bbox="841 982 1084 1012">• Spotlight on-device indexing <li data-bbox="841 1020 997 1050">• iOS Pairing Model <li data-bbox="841 1058 1006 1087">• Apple Configurator <li data-bbox="841 1096 945 1125">• Restrictions <li data-bbox="841 1134 1357 1184">• For more information about the security contents of iOS 9 see: support.apple.com/HT205212

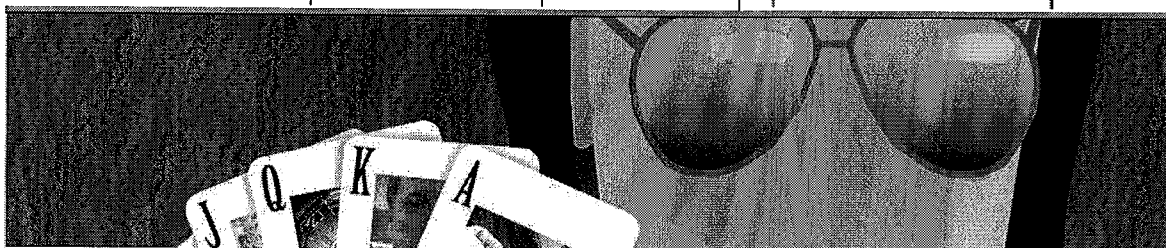
© 2015 Apple Inc. All rights reserved. Apple, the Apple logo, AirDrop, AirPlay, Apple TV, Apple Watch, Bonjour, FaceTime, iBooks, iMessage, iPad, iPhone, iPod, iPod touch, iTunes, Keychain, Mac, OS X, Safari, Siri, Spotlight, and Xcode are trademarks of Apple Inc., registered in the U.S. and other countries. Apple Pay, CarPlay Lightning, and Touch ID are trademarks of Apple Inc. iCloud and iTunes Store are service marks of Apple Inc., registered in the U.S. and other countries. App Store and iBooks Store are service marks of Apple Inc. iOS is a trademark or registered trademark of Cisco in the U.S. and other countries and is used under license. The Bluetooth® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by Apple is under license. Java is a registered trademark of Oracle and/or its affiliates. Other product and company names mentioned herein may be trademarks of their respective companies. Product specifications are subject to change without notice. September 2015

Exhibit B

3/2/2016

How cybercriminals use major news events to attack you

TOPICS ▾



Tech

How cybercriminals use major news events to attack you

By Patrick Howell O'Neill

Aug 5, 2013, 7:00am CT

<http://bit.ly/138XEhC>



Daily Dot Tech

Like Follow

A big news story always attracts big crowds. Inevitably, those crowds attract criminals looking to take advantage of the distracted and excited.

Cybercriminals are no different. They keep their finger on the pulse of trending news, using major events as a point of entry.

3/2/2016

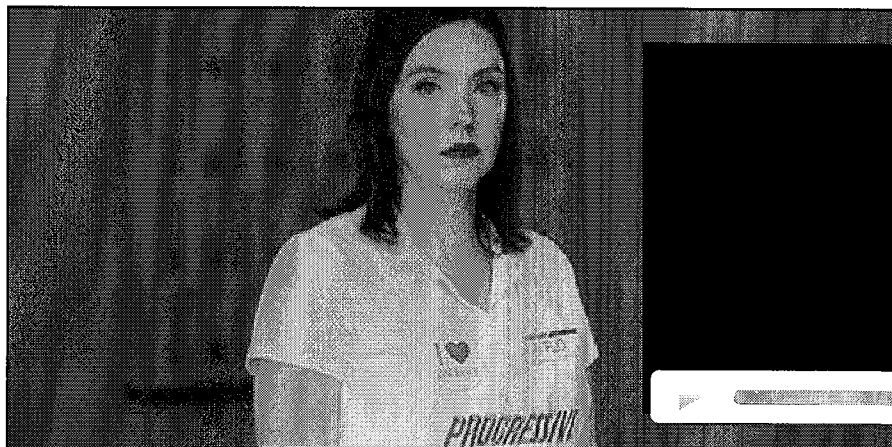
How cybercriminals use major news events to attack you

The recent birth of Prince George provides a perfect case study of the tactics often used and tips for avoiding hackers' tripwire links.

The watering hole attack

As millions of people searched for the latest news on the royal baby, emails promising a "live updates" and even an exclusive "hospital-cam" were reported by Kaspersky Lab in the hours leading up to and following the birth. The links, however, pointed to a once-legitimate but recently compromised and "trojanized" website infected with a Blackhole exploit kit—an originally Russian tool that has become one of the most prevalent hacking tools in existence today. Once a victim clicks the link, it triggers the download of malware such as a Zeus trojan virus, which is designed to log keystrokes and steal banking information.

ADVERTISEMENT



Action Fraud UK

recently warned against Twitter posts promising "#RoyalBabyBoy - Exclusive Pics!" In the U.S., the Better Business Bureau issued its own warning against Facebook friends liking "exclusive" videos of the new baby that can take curious clickers to dangerous websites.

3/2/2016

How cybercriminals use major news events to attack you

These are all popular variations of a powerfully effective tactic called a “watering hole attack,” in which hackers wait for victims to come to them instead of actively seeking them out. It’s named after the way a lion will wait for a thirsty water buffalo to inevitably arrive at a watering hole on a hot day. Then, she attacks.

Like thirsty animals, many of us are easily predictable herds in one circumstance or another. If the royal baby didn’t catch your attention, perhaps the recent controversy over Ender’s Game author Orson Scott Card’s anti-gay marriage activism did. While the royal baby was being born, malicious links disguised as CNN articles about a possible Ender’s Game boycott were inflicting the exact same watering hole attack on science-fiction fans that royal fans were enduring.

Major events such as the Super Bowl, Osama Bin Laden’s death, the Boston Marathon bombing, and the election of Pope Francis were used to push tempting links promising “exclusive” and a “new” videos in front of curious and excitable Web surfers. A single click can potentially lead to infection if the user’s anti-virus software proved out of date or inadequate—or if another program, such as Adobe Flash or Internet Explorer, was vulnerable (and they all too often are).

The scalpel approach

Using a global event such as the royal birth or Super Bowl to attack is deemed a “shotgun approach,” designed to infect millions of people around the globe. In contrast, some watering hole attacks can be targeted at specific organizations or individuals by simply adjusting the watering hole. The focused use of this tactic has been called “subtle and graceful” by Will Gragido, senior manager at RSA Security. As opposed to the shotgun, this sort of attacker is

3/2/2016

How cybercriminals use major news events to attack you

using a scalpel.

A highly sophisticated Chinese hacking group known as Elderwood was famously accused of stealing intellectual property from the likes of Google, Lockheed Martin, Dow Chemical and more in 2010's Operation Aurora using watering hole attacks. They have continued to use the tactic with increasing frequency and effectiveness, according to Symantec. The defense industry in particular has been infected repeatedly this way in the last year.

In July 2012, RSA FirstWatch reported on an attack called VOHO that compromised government websites, banks and human rights organizations. About 32,000 individuals visited the attack site, including 4,000 unique global organizations in state and federal government, academia, defense, and technology. The attack spread a Ghost Remote Access Trojan virus that has the ability to stealthily hijack and operate a victim's webcam, microphone, and ultimately, entire computer.

Likewise, in February 2013, hackers compromised the widely read iOS mobile developer forum called iPhoneDevSDK and used it to infect computers at Facebook, Apple and Twitter, reported Threatpost. The attackers knew who frequented that forum and, instead of attacking them head on, laid the trap at a favorite watering hole and eventually infected three tech giants.

ADVERTISEMENT

3/2/2016

How cybercriminals use major news events to attack you



Increasingly, hackers are attacking websites that employees and members of target organizations simply must use for work. Just as tech employees will often have to use a popular iOS mobile developer resource, government officials, journalists, businesses, and academics often have to access the website of the Council on Foreign Relations, one of the most influential think-tanks in Washington, D.C. When it was the target of a watering hole attack in for an entire week in December 2012, aggressors used a sophisticated "o-day" attack (i.e. an previously unknown method of attack) to put a wide range of globally influential organizations at risk of infection.

Many specifically targeted organizations are running into increasingly frequent and sophisticated o-day attacks that anti-virus programs have little to no defense against. Security officers and their employers across the private and public sectors have grown frustrated with this persistent and growing threat. Its growing use has been one of the key catalysts in the Obama administration's increasing focus on cybercrime and war.

While the likes of Google and Lockheed Martin have a lot to worry about, members of the general public will have a much easier time staying relatively safe for the simple fact that

3/2/2016

How cybercriminals use major news events to attack you

they're not worth as much money and effort.

The cheaper and often dated attacks targeting the public can generally be thwarted, according to the Better Business Bureau, by avoiding promotions of "exclusive" or outlandish videos or articles, always hovering over a link to make sure the URL is correct, and keeping all of your software—including anti-virus programs—up to date.

In short, be careful what you click.

Illustration by Jason Reed

<http://bit.ly/138XEhC>



Daily Dot Tech

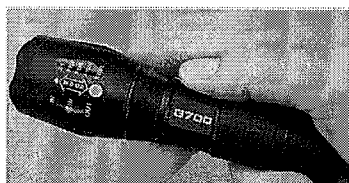
Like Follow

From the Web



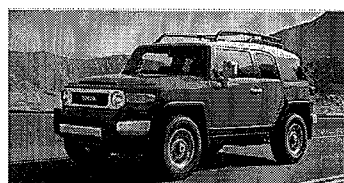
The Most Haunting Photos Too Horrifying To Be

Promoted by Check This, Yo!



"Worlds Brightest" Military Grade Flashlight Now

Promoted by Vir3



Top 10 Cars With the Highest Resale Value

Promoted by BuzzTicle

Exhibit C

3/2/2016

FBI Admits It Controlled Tor Servers Behind Mass Malware Attack | WIRED

SUBSCRIBE



KEVIN POULSEN SECURITY 09.13.13 4:17 PM

FBI ADMITS IT CONTROLLED TOR SERVERS BEHIND MASS MALWARE ATTACK

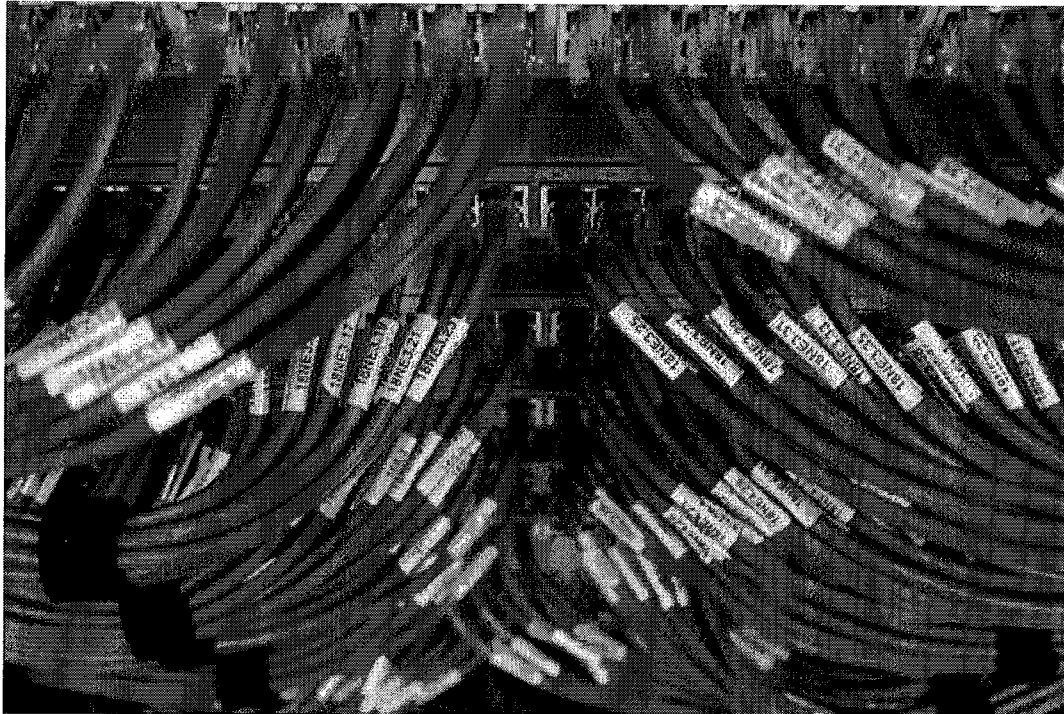


Photo: Andrew Hart/Flickr

IT WASN'T EVER seriously in doubt, but the FBI yesterday acknowledged that it secretly took control of Freedom Hosting last July, days before the servers of the largest provider of ultra-anonymous hosting were found to be serving custom malware designed to identify visitors.

Freedom Hosting's operator, Eric Eoin Marques, had rented the servers from an unnamed commercial hosting provider in France, and paid for

3/2/2016

FBI Admits It Controlled Tor Servers Behind Mass Malware Attack | WIRED

them from a bank account in Las Vegas. It's not clear how the FBI took over the servers in late July, but the bureau was temporarily thwarted when Marques somehow regained access and changed the passwords, briefly locking out the FBI until it gained back control.

The new details emerged in local press reports from a Thursday bail hearing in Dublin, Ireland, where Marques, 28, is fighting extradition to America on charges that Freedom Hosting facilitated child pornography on a massive scale. He was denied bail today for the second time since his arrest in July.

Freedom Hosting was a provider of turnkey "Tor hidden service" sites — special sites, with addresses ending in .onion, that hide their geographic location behind layers of routing, and can be reached only over the Tor anonymity network. Tor hidden services are used by sites that need to evade surveillance or protect users' privacy to an extraordinary degree — including human rights groups and journalists. But they also appeal to serious criminal elements, child-pornography traders among them.

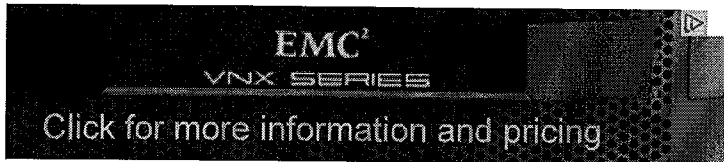
On August 4, all the sites hosted by Freedom Hosting — some with no connection to child porn — began serving an error message with hidden code embedded in the page. Security researchers dissected the code and found it exploited a security hole in Firefox to identify users of the Tor Browser Bundle, reporting back to a mysterious server in Northern Virginia. The FBI was the obvious suspect, but declined to comment on the incident. The FBI also didn't respond to inquiries from WIRED today.

But FBI Supervisory Special Agent J. Brooke Donahue was more forthcoming when he appeared in the Irish court yesterday to bolster the case for keeping Marques behind bars, according to local press reports. Among the many arguments Donahue and an Irish police inspector offered was that Marques might reestablish contact with co-conspirators, and further complicate the FBI probe. In addition to the wrestling match over Freedom Hosting's servers, Marques allegedly dove for his laptop when the police raided him, in an effort to shut it

3/2/2016

FBI Admits It Controlled Tor Servers Behind Mass Malware Attack | WIRED

down.



Donahue also said Marques had been researching the possibility of moving his hosting, and his residence, to Russia. “My suspicion is he was trying to look for a place to reside to make it the most difficult to be extradited to the U.S.,” said Donahue, according to the *Irish Independent*.

Freedom Hosting has long been notorious for allowing child porn to live on its servers. In 2011, the hactivist collective Anonymous singled out the service for denial-of-service attacks after allegedly finding the firm hosted 95 percent of the child porn hidden services on the Tor network. In the hearing yesterday, Donahue said the service hosted at least 100 child porn sites with thousands of users, and claimed Marques had visited some of the sites himself.

Reached by phone, Marques’ lawyer declined to comment on the case. Marques faces federal charges in Maryland, where the FBI’s child-exploitation unit is based, in a case that is still under seal.

The apparent FBI-malware attack was first noticed on August 4, when all of the hidden service sites hosted by Freedom Hosting began displaying a “Down for Maintenance” message. That included at least some lawful websites, such as the secure email provider TorMail.

Some visitors looking at the source code of the maintenance page realized that it included a hidden `iframe` tag that loaded a mysterious clump of Javascript code from a Verizon Business internet address. By midday, the code was being circulated and dissected all

3/2/2016

FBI Admits It Controlled Tor Servers Behind Mass Malware Attack | WIRED

over the net. Mozilla confirmed the code exploited a critical memory management vulnerability in Firefox that was publicly reported on June 25, and is fixed in the latest version of the browser.

Though many older revisions of Firefox were vulnerable to that bug, the malware only targeted Firefox 17 ESR, the version of Firefox that forms the basis of the Tor Browser Bundle - the easiest, most user-friendly package for using the Tor anonymity network. That made it clear early on that the attack was focused specifically on de-anonymizing Tor users.

Tor Browser Bundle users who installed or manually updated after June 26 were safe from the exploit, according to the Tor Project's security advisory on the hack.

```

589. function f(var15,view,var16)
590.
591.     var magneto = "";
592.     var magneto =
593.     ("Auc60Auee8" + "\u0000\u0000" + "\u0000\u0021"
594.     var var23 = magneto;
595.     var var17 = "\u0061";
596.     var var18 = "\u0041\u0000\u0000";
597.     var var20 = "\u2552\u2000" + String.fromCharCode
598.     var var21 = "\u2552\u2000" + String.fromCharCode
599.     var var22 = "\u0089";
600.     var var23 = "\u0000";
601.     var var24 = "\u0089";
602.     var24 += "\u0000\u0000";

```

The payload for the Tor Browser Bundle malware is hidden in a variable called "magneto."

Perhaps the strongest evidence that the attack was a law enforcement or intelligence operation was the limited functionality of the malware.

The heart of the malicious Javascript was a tiny Windows executable hidden in a variable named "Magneto." A traditional virus would use that executable to download and install a full-featured backdoor, so the hacker could come in later and steal passwords, enlist the computer in a DDoS botnet, and generally do all the other nasty things that happen to a hacked Windows box.

But the Magneto code didn't download anything. It looked up the victim's MAC address — a unique hardware identifier for the

3/2/2016

FBI Admits It Controlled Tor Servers Behind Mass Malware Attack | WIRED

computer's network or Wi-Fi card — and the victim's Windows hostname. Then it sent it to a server in Northern Virginia server, bypassing Tor, to expose the user's real IP address, coding the transmission as a standard HTTP web request.

“The attackers spent a reasonable amount of time writing a reliable exploit, and a fairly customized payload, and it doesn't allow them to download a backdoor or conduct any secondary activity,” said Vlad Tsvrklevich, who reverse-engineered the Magneto code, at the time.



The malware also sent a serial number that likely ties the target to his or her visit to the hacked Freedom Hosting-hosted website.

The official IP allocation records maintained by the American Registry for Internet Numbers show the two Magneto-related IP addresses were part of a ghost block of eight addresses that have no organization listed. Those addresses trace no further than the Verizon Business data center in Ashburn, Virginia, 20 miles northwest of the Capital Beltway.

The code's behavior, and the command-and-control server's Virginia placement, is also consistent with what's known about the FBI's “computer and internet protocol address verifier,” or CIPAV, the law enforcement spyware first reported by WIRED in 2007.

Court documents and FBI files released under the FOIA have described the CIPAV as software the FBI can deliver through a browser exploit to gather information from the target's machine and send it to an FBI server in Virginia. The FBI has been using the CIPAV since 2002 against hackers, online sexual predators, extortionists, and others, primarily to identify suspects who are disguising their location using proxy servers

3/2/2016

FBI Admits It Controlled Tor Servers Behind Mass Malware Attack | WIRED


or anonymity services, like Tor.

Prior to the Freedom Hosting attack, the code had been used sparingly, which kept it from leaking out and being analyzed.


No date has been set for Marques' extradition hearings, but it's not expected to happen until next year.

VIEW COMMENTS


SPONSORED STORIES




MONEY SHORT CUTS
Advice bailiffs don't want you to know




OPEN TABLE
Why the Country's Top Restaurants Are Eliminating Tips



LOLBOOM
Python Eats A Porcupine Whole Then Something Unreal Happens



VIRALMOZO
17 Times Google Maps Has Caught Disturbing Images



DVD ENERGY
This simple trick could cut your energy bills by £160

POWERED BY OUTBRAIN

Exhibit D

The Washington Post

National Security

Meet the woman in charge of the FBI's most controversial high-tech tools

By Ellen Nakashima December 8, 2015

In the aftermath of Wednesday's shooting rampage in San Bernardino, FBI teams recovered computer hard drives, flash drives and crushed cellphones left by the attackers. They flew the evidence to technical sleuths at a special FBI facility in Northern Virginia. At the same time, a crew from the bureau's lab there jetted to California to help reconstruct the shooting.

The tragedy in California is the latest big case that involves the mostly unseen scientists who work for the FBI's Amy Hess in Quantico, Va. She is the FBI's executive assistant director for science and technology, the master of much that is cool — and controversial — in the bureau's arsenal of high-tech tools.

At Quantico on any given day, you might see FBI technicians pick apart a cellphone flown in from an overseas battlefield. Or robots processing DNA samples from convicted felons. Or in a room as large as a football field, scientists testing the signal strength of a radio antenna.

But even as it is developing biometric databases, rapid DNA-matching machines and laser-beam imagery for ballistic purposes — or trying to extract data from crushed cellphones that might offer insight into the San Bernardino shooters' motives — the FBI is struggling to meet ever more complex technological challenges.

In cyber investigations, a crucial part of the bureau's work, current and former agents say that the Operational Technology Division, or OTD, which Hess oversees, has failed to provide adequate tools to analyze massive amounts of digital data in hacking and cyberspying cases.

And despite the wizardry of its technologists, who also excel at traditional physical and electronic surveillance, the bureau is at a loss to solve what FBI Director James B. Comey has called one of the most worrisome problems facing law enforcement today: the advent of strong commercial encryption on cellphones where only the user can unlock the data.

At the same time, the bureau is facing concerns that the technologies it deploys — cellphone tracking, computer hacking and facial and iris recognition — lack sufficient protections for citizens' privacy.

Hess says she considers it a privilege to be where she is. "When I'm sitting in the morning meetings with the director and deputy director, I know that the folks in my branch somehow contributed to the big case we're all talking about that day," she said.

Born and raised in a suburb of Louisville, Hess, 49, entered the FBI Academy in 1991, the second-youngest in her class, a good athlete and a whiz at video games.

“Even though my parents were essentially pacifists, we didn’t have guns in the house, I learned hand-eye coordination to the point where I got the Top Gun award for my [new agents’] class,” she said.

Hess, who has an astronautical engineering degree, started in the bureau’s science and engineering program. But her career path also took her into traditional cops-and-robbers investigations and domestic and international terrorism cases, including stints at headquarters and in Afghanistan.

In 2014, she was tapped to head science and technology. She has more people working for her — about 6,000 — than any other FBI branch. Her branch also has the single largest budget — somewhere between \$600 million and \$800 million. The bureau will not say how much.

Critical investigative support

Hess’s branch is rarely in the limelight, but the scientists at OTD and the laboratory, and at the Criminal Justice Information Services Division in Clarksburg, W.Va., provide crucial support to the government’s investigations and prosecutions.

“Whatever needs to be done — anything from evidence response to being able to sort through volumes of video and photographs — her branch is absolutely foundational to any kind of investigative success,” said Stephanie Douglas, a former executive assistant director of the FBI’s National Security Branch.

When the 2013 Boston Marathon was disrupted by deadly bomb explosions, OTD forensic analysts, as well as field office personnel, pored over hours of disparate video footage flooding in from restaurant and bar surveillance systems, television cameras and bystanders’ cellphones. They were able to stitch together a pivotal sequence. That video, never shown to the public in its entirety, captures a tall man with a white baseball cap walking through the crowd and casually placing a backpack on the sidewalk. The sound of an explosion — it was the first bomb — startles bystanders, who look to the left. The man just stands there, then walks off, leaving his backpack. Seconds later, the backpack explodes, killing an 8-year-old boy and severing a leg of the boy’s younger sister. That heart-wrenching video was shown privately to the jury, which convicted Dzhokhar Tsarnaev.

Also that year, when a gunman in Alabama took a 5-year-old boy hostage for a week in an underground bunker on his property, OTD devised a way to get eyes on the kidnapper. Technicians, working with the bureau’s hostage rescue team, hid an audio-video camera in a stuffed toy dinosaur, and the rescue team persuaded the abductor to pass it to the boy. The surveillance showed what was going on in the bunker and facilitated the child’s rescue.

The advent of strong encryption, however, is presenting Hess with a huge, perhaps insurmountable, challenge.

In the past few years, tech firms and app developers have increasingly built platforms that employ a form of encryption that only the user, not the company, can unlock.

The bureau's encryption dilemma is exacerbated by a chill that settled over the relationship between the FBI and Silicon Valley in the wake of leaks in 2013 about government surveillance by former National Security Agency contractor Edward Snowden.

Firms that feared being tagged as tools of a privacy-invading government became less willing to assist in surveillance "because it was perceived as not a good business model to be seen as cooperating with the government," Hess said.

It used to be, she said, that companies meeting a legal requirement to provide "technical assistance" generally would try to comply with wiretap orders. "Now all of a sudden we get hung up on the question of what, exactly, does that mean I have to provide to you?" she said.

In recent months, the FBI's conversations with companies have become more productive, she said, "but it's not to the level we were pre-Snowden."

Another challenge lies in cyberspace. Investigating intrusions, whether by Russian or Eastern European crime rings or Chinese government hackers, has become one of the FBI's most important tasks. But agents in the field — techies who live and breathe ones and zeroes — say that tools provided by the OTD fall short.

The problem, they say, is a platform built to analyze data for counterterrorism and criminal probes. Insight, as it is called, can track the websites a suspect has visited, pull emails from a suspect's account and reconstruct deleted emails. But the agents say it chokes on large amounts of network data.

In at least one case, an investigation has died as a result. And some agents have created their own tools or bought them commercially.

“For 30 years, OTD has been awesome at wiring up agents, putting micro-cameras on people, wiring up cars,” said one individual who, like several others, spoke on the condition of anonymity to be candid. “Where they suffer is understanding cyber investigations and cyber agents’ needs.”

Senior FBI officials say a fix is on the way. The cyber division has given OTD several million dollars to modify Insight. But that fix could take six months to a year, officials said.

‘High-tech and creepy’

More than any other FBI executive, Hess must navigate the tension between privacy and security.

While she might be seen as a kind of female Q, head of the fictional spy agency Skunkworks in the James Bond movies, Christopher Soghoian, principal technologist at the American Civil Liberties Union, sees her as “the queen of domestic surveillance.”

Said Soghoian: “All of the most interesting and troubling stuff that the FBI does happens under Amy Hess.” Whether it’s turning on the taps to collect data from tech companies to pass to the NSA (under court order), or covertly entering people’s houses to install bugs (with a warrant), he said, “if it’s high-tech and creepy, it’s happening in the Operational Technology Division.”

One area of controversy is the bureau’s use of cell site simulators, or StingRays, which mimic cellphone towers to elicit signals from cellphones in an area, including from innocent bystanders. The FBI has long been secretive about the tool’s use, and has even made state and local law enforcement sign nondisclosure agreements.

Though the agreements typically state that the local agency “will not . . . disclose any information concerning” the equipment, Hess insists that the FBI has never imposed a gag on local police. For the record, she said, the bureau does not object to revealing the use of the device. It’s the “engineering schematics,” details on exactly how the tool works, that the FBI wants shielded, she said.

Another group that remains shrouded is OTD's Remote Operations Unit. There, technicians with a warrant hack computers to identify suspects. Euphemistically called "network investigative techniques," that activity has stirred concerns similar to those raised with the use of StingRays.

For one thing, the warrant applications do not describe the technique's use in detail. So judges may not really understand what they are authorizing. Hess said that agents can describe the process more fully to a judge in closed chambers. That's if the judge knows to ask.

Privacy advocates also worry that to carry out its hacks, the FBI is using "zero-day" exploits that take advantage of software flaws that have not been disclosed to the software maker. That practice makes consumers who use the software vulnerable, they argue.

Hess acknowledged that the bureau uses zero-days — the first time an official has done so. She said the trade-off is one the bureau wrestles with. "What is the greater good — to be able to identify a person who is threatening public safety?" Or to alert software makers to bugs that, if unpatched, could leave consumers vulnerable?

"How do we balance that?" she said. "That is a constant challenge for us."

She added that hacking computers is not a favored FBI technique. "It's frail," she said. As soon as a tech firm updates its software, the tool vanishes. "It clearly is not reliable" in the way a traditional wiretap is, she said.

Confident of finding solutions

On a recent afternoon, Hess stood in a warehouse-like space set apart from the four-story lab. There, she surveyed boxes of terrorist bomb-making materials — switches, batteries, pressure plates — resting on pallets and waiting to be examined by FBI scientists.

Every piece is meticulously analyzed, photographed and cross-referenced in a database. Fingerprints and DNA are lifted. Trace chemicals are assayed. Components are scrutinized. That way the FBI can match, say, a particular type of wire used to a specific terrorist cell in Yemen.

Since 2003, the Terrorist Explosive Device Analytical Center has collected close to a million individual pieces of terrorist-bomb evidence: the explosive hidden in the underwear of a militant seeking to blow up a Detroit-bound jet, the remnants of the Boston Marathon bombs, the shards of roadside explosives that have killed and maimed thousands of American troops in Iraq and Afghanistan.

It is the scale and depth of the technical work done by her branch that makes Hess confident about finding solutions the problems that have yet to be solved.

"I don't think my job is to sit on the porch and watch it all go by and say, 'Ah, that's too hard,'" she said. "My job

is to get off the porch, get in the middle of the problem and say, 'We have an obligation to the American public to protect public safety and to prevent threats from happening.'"

Ellen Nakashima is a national security reporter for The Washington Post. She focuses on issues relating to intelligence, technology and civil liberties.

Exhibit E

The Washington Post

The Switch

Forbes Web site was compromised by Chinese cyberespionage group, researchers say

By Andrea Peterson February 10, 2015

Chinese hackers hijacked Forbes.com and used the site as part of an attack on the U.S. defense and financial industry, according to cybersecurity researchers at iSIGHT Partners and Invincea.

For three days late last year, the news site's "Thought of the Day" widget, which appears when readers visit the site, was compromised — seamlessly redirecting visitors from certain organizations to another site where their computers could be infected with malware without their knowledge.

Researchers have linked similar malware controlled by the same server used in the Forbes attack to breaches of Web sites frequented by domestic Chinese dissident groups.

Forbes acknowledged the incident. "On December 1, 2014, Forbes discovered that on November 28, 2014, a file had been modified on a system related to the Forbes web site," the outlet said in a statement to The Post. "The file was immediately reverted and an investigation by Forbes into the incident began. Forbes took immediate actions to remediate the incident." The news outlet's investigation found "no indication of additional or ongoing compromise nor any evidence of data exfiltration," according to the statement.

The hack comes amid growing concerns that even the most trusted sites can be used by hackers aimed at infiltrating sensitive industries. The White House is creating a new agency focused on coordinating the government's response to the deepening threat from cyberattacks, according to a Washington Post report Thursday.

Using Forbes.com was "fairly brazen" and a shrewd move, Steve Ward, senior director at iSIGHT Partners, told the the Post in an interview. "It's a trusted place that all of the employees in a targeted organization are going to be allowed to go to," he explained. "It's not going to be blocked from inside. "

"It's sort of a compliment to Forbes, but kind of a backhanded compliment," said James A. Lewis, a senior fellow at the Center for Strategic and International Studies. "They thought 'interesting people go to Forbes, and that Forbes is a site we can get into,'" he explained.

The attack worked by leveraging two undisclosed coding flaws — typically called "zero day" vulnerabilities. The first was a problem with Adobe Flash, which the company patched December 9th, and the second was an Internet Explorer flaw, which Microsoft released a fix for on Tuesday. The Internet Explorer flaw was deployed

by the attackers when the the Flash flaw alone was not enough to compromise targeted visitors' systems.

The hack redirected some of the site's visitors to a malicious site where their computers were silently attacked by malware. The researchers said they believe the malware was only used to infect a select group of targets, despite the broad audience of Forbes.com, which is ranked among the top 200 most visited sites globally by Alexa. The researchers said they confirmed the attack targeted at least some companies within the defense and financial services industries although it's possible its reach was larger.

Invincea, a cybersecurity monitoring company, said that they determined in late November that one of their defense industry clients had been targeted by the attack. They were able to stop the malware from spreading inside the client's network and collected forensic data that helped it determine the origin of the attack, company officials said.

The researchers attributed the hack to a cyberespionage group called Team Codoso, also known as the Sunshop Group, which has a long history of similar "watering hole" style attacks. Researchers at FireEye linked the group to attacks affecting multiple Korean military and strategy think tanks and a Uighur news and discussion site, among others, in 2013.

"When you talk to the Chinese, they tell you the U.S. is priority number two," said Lewis. "Priority number one is domestic political stability, so that's where they focus the bulk of their efforts."

Chinese groups have been blamed for a widespread cyberespionage campaign against the U.S. government and American businesses reaching back several years. The recent breach at health-insurer Anthem is suspected to be linked to Chinese hackers.

Nearly every major news outlet, including the Washington Post and the New York Times, have reported that they were victims of attacks suspected to be carried out by Chinese hackers — but the Forbes attack shows that security vulnerabilities at outlets can also put readers at risk.

Andrea Peterson covers technology policy for The Washington Post, with an emphasis on cybersecurity, consumer privacy, transparency, surveillance and open government.

Market Watch

DJIA **2.11%**
NASDAQ **2.89%**

Last Update:
03/02/2016(DJIA&NASDAQ)

Exhibit F

DATA AND GOLIATH

The Hidden Battles to Collect
Your Data and Control Your World

BRUCE SCHNEIER



W. W. NORTON & COMPANY
NEW YORK • LONDON

As of press time, the URLs displayed in this book link or refer to existing websites on the Internet. W. W. Norton & Company is not responsible for, and should not be deemed to endorse or recommend, any website other than its own or any content available on the Internet (including without limitation at any website, blog page, information page) not created or maintained by W. W. Norton.

Copyright © 2015 by Bruce Schneier

All rights reserved
Printed in the United States of America
First Edition

For information about permission to reproduce selections from this book, write to Permissions, W. W. Norton & Company, Inc., 500 Fifth Avenue, New York, NY 10110

For information about special discounts for bulk purchases, please contact W. W. Norton Special Sales at specialsales@wnorton.com or 800-233-4830

Manufacturing by RR Donnelley Harrisonburg
Book design by Daniel Lagin
Production manager, Julia Druskin

ISBN: 978-0-393-24481-6

W. W. Norton & Company, Inc.
500 Fifth Avenue, New York, N.Y. 10110
www.wnorton.com

W. W. Norton & Company Ltd.
Castle House, 75/76 Wells Street, London W1T 3QT

2 3 4 5 6 7 8 9 0

THE PREVALENCE OF VULNERABILITIES

Vulnerabilities are mistakes. They're errors in design or implementation—glitches in the code or hardware—that allow unauthorized intrusion into a system. So, for example, a cybercriminal might exploit a vulnerability to break into your computer, eavesdrop on your web connection, and steal the password you use to log in to your bank account. A government intelligence agency might use a vulnerability to break into the network of a foreign terrorist organization and disrupt its operations, or to steal a foreign corporation's intellectual property. Another government intelligence agency might take advantage of a vulnerability to eavesdrop on political dissidents, or terrorist cells, or rival government leaders. And a military might use a vulnerability to launch a cyberweapon. This is all hacking.

When someone discovers a vulnerability, she can use it either for defense or for offense. Defense means alerting the vendor and getting it patched—and publishing it so the community can learn from it. Lots of vulnerabilities are discovered by vendors themselves and patched without any fanfare. Others are discovered by researchers and ethical hackers.

Offense involves using the vulnerability to attack others. Unpublished vulnerabilities are called "zero-day" vulnerabilities; they're very valuable to attackers because no one is protected against them, and they can be used worldwide with impunity. Eventually the affected software's vendor finds out—the timing depends on how widely the vulnerability is exploited—and issues a patch to close it.

If an offensive military cyber unit or a cyberweapons manufacturer discovers the vulnerability, it will keep it secret for future use to build a cyberweapon. If used rarely and stealthily, the vulnerability might remain secret for a long time. If unused, it will remain secret until someone else discovers it.

Discoverers can sell vulnerabilities. There's a robust market in zero-days for attack purposes—both governments and cyberweapons manufacturers that sell to governments are buyers—and black markets where discoverers can sell to criminals. Some vendors offer bounties for vulnerabilities to spur defense research, but the rewards are much lower.

Undiscovered zero-day vulnerabilities are common. Every piece of

146 DATA AND GOLIATH

commercial software—your smartphone, your computer, the embedded systems that run nuclear power plants—has hundreds if not thousands of vulnerabilities, most of them undiscovered. The science and engineering of programming just isn't good enough to produce flawless software, and that isn't going to change anytime soon. The economics of software development prioritize features and speed to market, not security.

What all this means is that the threat of hacking isn't going away. For the foreseeable future, it will always be possible for a sufficiently skilled attacker to find a vulnerability in a defender's system. This will be true for militaries building cyberweapons, intelligence agencies trying to break into systems in order to eavesdrop, and criminals of all kinds.

MAINTAINING AN INSECURE INTERNET

In Chapter 6, I discussed how the NSA uses both existing and specially created vulnerabilities to hack into systems. Its actions put surveillance ahead of security, and end up making us all less secure. Here's how the NSA and GCHQ think, according to a *Guardian* article on some of the Snowden documents: "Classified briefings between the agencies celebrate their success at 'defeating network security and privacy...'"

Just how do governments go about defeating security and privacy? We know the NSA uses the following four main practices. Assume that the Russians, Chinese, and various other countries are using similar methods. And cybercriminals aren't far behind.

Stockpiling vulnerabilities in commercial software that we use every day, rather than making sure those security flaws get fixed. When the NSA discovers (or buys) a vulnerability, it can either alert the vendor and get a still-secret vulnerability fixed, or it can hold on to it and use it to eavesdrop on target computer systems. Both tactics support important US policy goals, but the NSA has to choose which one to pursue in each case.

Right now, the US—both at the NSA and at US Cyber Command—stockpiles zero-day vulnerabilities. How many it has is unclear. In 2014, the White House tried to clarify the country's policy on this in a blog post, but didn't really explain it. We know that a single cyberweapon, Stuxnet, used four zero-days. Using up that many for a single cyberattack implies that the government's stockpile is in the hundreds.

Exhibit G

LIBERTY AND SECURITY IN A CHANGING WORLD

12 December 2013

**Report and Recommendations of
The President's Review Group on Intelligence
and Communications Technologies**

of US person data and a prohibition on using data that is beyond authorized retention limits.

Recommendation 30

We recommend that the National Security Council staff should manage an interagency process to review on a regular basis the activities of the US Government regarding attacks that exploit a previously unknown vulnerability in a computer application or system. These are often called "Zero Day" attacks because developers have had zero days to address and patch the vulnerability. US policy should generally move to ensure that Zero Days are quickly blocked, so that the underlying vulnerabilities are patched on US Government and other networks. In rare instances, US policy may briefly authorize using a Zero Day for high priority intelligence collection, following senior, interagency review involving all appropriate departments.

NSA and other US Government agencies, such as DHS, have important missions to assist US corporations in the protection of privately owned and operated critical infrastructure information networks. To do so, NSA, DHS, and other agencies should identify vulnerabilities in software widely employed in critical infrastructure and then work to eliminate those vulnerabilities as quickly as possible. That duty to defend, however, may sometimes come into conflict with the intelligence collection mission, particularly when it comes to what are known as "Zero Days."

A Zero Day or "0 Day" exploit is a previously unknown vulnerability in software in a computer application or system - the developers or system

owners have had zero days to address or patch the vulnerability. Because the software attack technique has not been used or seen before, it enables a cyber attacker to penetrate a system or to achieve other malicious goals. In almost all instances, for widely used code, it is in the national interest to eliminate software vulnerabilities rather than to use them for US intelligence collection. Eliminating the vulnerabilities—“patching” them—strengthens the security of US Government, critical infrastructure, and other computer systems.

We recommend that, when an urgent and significant national security priority can be addressed by the use of a Zero Day, an agency of the US Government may be authorized to use temporarily a Zero Day instead of immediately fixing the underlying vulnerability. Before approving use of the Zero Day rather than patching a vulnerability, there should be a senior-level, interagency approval process that employs a risk management approach. The NSS should chair the process, with regular reviews. All offices and departments with relevant concerns, generally including the National Economic Council, State, Commerce, Energy, and Homeland Security, should be involved in that process.

D. Institutional Measures for Cyberspace

Recommendation 31

We recommend that the United States should support international norms or international agreements for specific measures that will increase confidence in the security of online communications. Among those measures to be considered are:

Exhibit H



MOBILE SECURITY TIP CARD

Mobile devices enable Americans to get online wherever they are. It's important to understand how to protect yourself when connecting on the go.

DID YOU KNOW?

- **Fifty-six percent** of all people own a smartphone.¹
- **Eighty percent of time spent** on a mobile device is inside apps.²
- Of all emails opened, nearly **30% are opened on a mobile device.**³
- In 2011, **31% of mobile users** received a text from someone they didn't know asking them to click on an embedded link.⁴
- In a study, **59% of respondents saw a jump in malware infections** due to unsecure mobile devices.⁵

SIMPLE TIPS

1. Restrict access to your wireless network by only allowing authorized users access to your network.
2. Change any pre-configured default passwords on your mobile device to ones that would be difficult for an outsider to guess.
3. Keep your anti-virus software updated.
4. Use caution when downloading or clicking on any unknown links.
5. Use your mobile device carefully; emails that can harm your computer can also harm your mobile device.
6. Be sure to review and understand the details of an app before installing it and be wary of the information it requests.

Use the Federal Communications Commission's mobile phone security checker at www.fcc.gov/smartphone-security.

1 Super Monitoring, State of Mobile 2013

2 Ibid.

3 Ibid.

4 Symantec, 2013 Norton Cybercrime Report

5 Ponemon Institute, Global Study on Mobility Risks, 2012

MOBILE SECURITY TIP CARD



RESOURCES AVAILABLE TO YOU

US-CERT.gov

US-CERT provides tips for both individuals and organizations on how to protect against cyber threats. Visit www.us-cert.gov/cas/tips/ for more information.

Justice.gov

The Department of Justice Computer Crime and Intellectual Property Section tells you where to report hacking, password trafficking, spam, child exploitation and other Internet harassment. Visit www.justice.gov/criminal/cybercrime/ for more information.

OnGuardOnline.gov

This website, run by the Federal Trade Commission, is a one-stop shop for online safety resources available to individuals of all ages.

StaySafeOnline.org

The National Cyber Security Alliance offers instruction on security updates, free anti-virus software, malware software removal and other services.

IF YOU ARE A VICTIM OF ONLINE CRIME

- Immediately notify your local authorities and file a complaint with the Internet Crime Complaint Center at www.ic3.gov.
- If you think a site has collected your personal information in a way that violates the law, report it to the FTC at www.ftc.gov/complaint.
- If someone has had inappropriate contact with you or a colleague, report it to www.cybertipline.com and they will coordinate with the FBI and local authorities.

Stop.Think.Connect.™ is a national public awareness campaign aimed at empowering the American public to be safer and more secure online. The Campaign's main objective is to help you become more aware of growing cyber threats and arm you with the tools to protect yourself, your family and your community. For more information visit www.dhs.gov/stopthinkconnect.



**Homeland
Security**

www.dhs.gov/stopthinkconnect



STOP | THINK | CONNECT™

Exhibit I



1900 M Street, NW, Ste. 250, Washington, D.C. 20036
marc@zwillgen.com

Marc J. Zwillinger
(202) 706-5202 (phone)
(202) 706-5298 (fax)

February 17, 2016

VIA ELECTRONIC FILING – UNDER SEAL

The Honorable James Orenstein
United States Magistrate Judge
United States District Court
Eastern District of New York
225 Cadman Plaza East
Brooklyn, NY 11201

Re: *In re Order Requiring Apple Inc. to Assist in the Execution of a Search Warrant
Issued by the Court, No. 15-MC-1902*

Dear Judge Orenstein:

I write in response to this Court's February 16, 2016 order (the "Order") requesting that Apple provide certain additional details regarding other requests it has received during the pendency of this matter that are of a similar nature to the one at issue in the instant case.

As recently as yesterday, Apple was served with an order by the United States Attorney's Office for the Central District of California. (*See Exhibit A.*) The government obtained that order on the basis of an *ex parte* application pursuant to the All Writs Act (*see Exhibit B*), regarding which Apple had no prior opportunity to be heard (despite having specifically requested from the government in advance the opportunity to do so). The attached order directs Apple to perform even more burdensome and involved engineering than that sought in the case currently before this Court—*i.e.*, to create and load Apple-signed software onto the subject iPhone device to circumvent the security and anti-tampering features of the device in order to enable the government to hack the passcode to obtain access to the protected data contained therein. (*See Exhibit A.*) As invited by the California court's order, Apple intends to promptly seek relief. But, as this recent case makes apparent, the issue remains quite pressing.

In addition to the aforementioned order, Apple has received other All Writs Act orders during the pendency of this case, certain details of which are set forth in the table below. In particular, for each such request Apple provides the following categories of information requested in the Order:

(1) the jurisdiction in which the request was made, (2) the type of device at issue in the request, (3) the version of iOS being used on that device, and (4) Apple's response to the request and/or its current status, as applicable.

Date Received	Jurisdiction	Device Type	iOS Version	Status
10/8/2015	Southern District of New York	iPhone 4S	7.0.4	Apple objected (12/9/2015)
10/30/2015	Southern District of New York	iPhone 5S	7.1	Apple objected (12/9/2015)
11/16/2015	Eastern District of New York	iPhone 6 Plus	8.1.2	Apple objected (12/9/2015)
		iPhone 6	8.1.2	
11/18/2015	Northern District of Illinois	iPhone 5S	7.1.1	Apple objected (12/9/2015)
12/4/2015	Northern District of California	iPhone 6	8.0 (or higher)	Apple objected (12/9/2015)
		iPhone 3	4.2.1	
		iPhone 3	6.1.6	
12/9/2015	Northern District of Illinois	iPhone 5S	7.0.5	Apple requested copy of underlying Motion but has not received it yet (2/1/2016)
1/13/2016	Southern District of California	N/A (device ID not yet provided)	N/A (device ID not yet provided, but the requesting agent advised device is pre-iOS 8)	Apple was advised by the requesting agent that she is seeking a new warrant. Apple has not yet received this warrant.
2/2/2016	Northern District of Illinois	iPad 2 Wifi	7.0.6	Apple objected (2/5/2016)
2/9/2016	District of Massachusetts	iPhone 6 Plus	9.1	Apple objected (2/11/2016)

With respect to the other categories of information sought in the Order (specifically, categories 4-6), Apple responds that following its objection or other response to each request there has not been any final disposition thereof to Apple's knowledge, and Apple has not agreed to perform any services on the devices to which those requests are directed.¹

Sincerely,

/s/ Marc J. Zwillinger

Marc J. Zwillinger

cc: All Counsel of Record (via ECF)

¹ Apple further notes that shortly preceding the pendency of the instant case, it received additional All Writs Act orders—specifically, two from the Southern District of Ohio (both on September 24, 2015) and Northern District of Illinois (on October 6, 2015). Apple objected to each of these orders, and to Apple's knowledge there have been no further developments since such objections were lodged.

Exhibit J

3/2/2016

Slippery Slope? Court Orders Apple To Unlock Shooter's iPhone : NPR



TECHNOLOGY

Slippery Slope? Court Orders Apple To Unlock Shooter's iPhone

Updated February 19, 2016 · 1:38 PM ET

Published February 18, 2016 · 5:15 AM ET



MARTIN KASTE

Listen to the Story

Morning Edition

4:01

Embed

Transcript

Apple says it would fight a federal court order to help the FBI break into a dead terrorist's iPhone. The feds say they're being kept out by one of the phone's security features.

RENEE MONTAGNE, HOST:

Apple says it will fight a federal court order to help the FBI break into an iPhone. Specifically, it is the phone used by Syed Farook, one of the two terrorists who killed 14 people in San Bernardino, Calif. The feds say they can't access the phone because of Apple's security features. Apple calls the court order government overreach, arguing it threatens the privacy of all its customers.

NPR's Martin Kaste has more.

MARTIN KASTE, BYLINE: This fight's been brewing for more than a year, since the fall of 2014 when Apple rolled out a new operating system for the iPhone with encryption so good that even Apple wouldn't be able to open it without the owner's password. Cyrus Vance, Jr. says that made his job harder. He's the district attorney in

3/2/2016

Slippery Slope? Court Orders Apple To Unlock Shooter's iPhone : NPR

Manhattan, and his evidence department now has a growing inventory of unopenable iPhones.

CYRUS VANCE JR.: We now have about 155 to 160 devices that are running on iOS 8 that are blocked and we can't get in them.

KASTE: They can't get in, even with a warrant. Permission from a judge is beside the point because Apple simply can't comply. Vance has been campaigning against the company's policy for months. He says a mature company would feel a responsibility to help with public safety.

VANCE: They're taking the opposite approach and acting like teenagers saying you can't tell me what to do, no matter how important the public safety imperative is.

KASTE: And this is why the law enforcement world is celebrating the FBI's showdown with Apple over the phone from San Bernardino. The feds are essentially saying - OK, Apple. You say you can't open this phone, but you still have to help us.

ROBERT CATTANACH: The government is very strategic in doing two things. It picked a very high profile, very emotional case, and what it requested was very narrow.

KASTE: That's Robert Cattanach, a former Justice Department attorney who now specializes in cybersecurity. He says the FBI is just asking Apple to write a piece of custom software that'll keep the phone from wiping its data while the feds use their own methods to try to hack in. It seems like a small favor to ask, and Cattanach says that's the point.

CATTANACH: Once you take this step, if you are Apple - and I - there are all sorts of reasons why they're not going to take this step willingly. But then what's the next step and the next step? Then where do you draw the line?

KASTE: In other words, this could be the start of a slippery slope, with the government asking for one small technical favor after another. Apple CEO Tim Cook certainly sees it that way. In a letter to customers, he said it could lead to government requests for Apple to write surveillance software or to track phone locations. That fear has privacy advocates rallying to Apple's side.

3/2/2016

Slippery Slope? Court Orders Apple To Unlock Shooter's iPhone : NPR

Christopher Soghoian is the ACLU's principal technologist. He says people in law enforcement seem to think that they should never be completely locked out of any technology.

CHRISTOPHER SOGHOIAN: They think that it's reasonable that people have a fight about what piece of paper the government gets - whether they get a warrant, whether they get a wiretap order, whether they get a subpoena - but that ultimately every single bit of information should be available to the government. And then I think there are many people in the civil liberties community who think that, in fact, that it should be possible to have a conversation that the government can never listen to.

KASTE: Pete Modafferi is the chief of detectives for the district attorney's office in Rockland County, N.Y., and he's been analyzing the effects of growing encryption for the International Association of Chiefs of Police. In recent years, cell phones have become key for police work. He says a detective is lucky when he finds one at a crime scene. And that's why he's puzzled by the people who are taking Apple's side in this.

PETE MODAFFERI: But I can't understand why people are so upset about the possibility of law enforcement using legal process to get access to this evidence. We're not after John Q. Public. We're really after criminals, and I don't think they understand the magnitude of what they're doing to us.

KASTE: For law enforcement agencies who share this view, the FBI's request for help in the San Bernardino case has the potential of swinging public opinion back toward the cops' point of view.

Martin Kaste, NPR News.

Copyright © 2016 NPR. All rights reserved. Visit our website terms of use and permissions pages at www.npr.org for further information.

NPR transcripts are created on a rush deadline by a contractor for NPR, and accuracy and availability may vary. This text may not be in its final form and may be updated or revised in the future. Please be aware that the authoritative record of NPR's programming is the audio.



© 2016 npr

SHARE

<http://www.npr.org/2016/02/18/467176553/slippy-slope-court-orders-apple-to-unlock-shooter-s-iphone>

3/4

Exhibit K

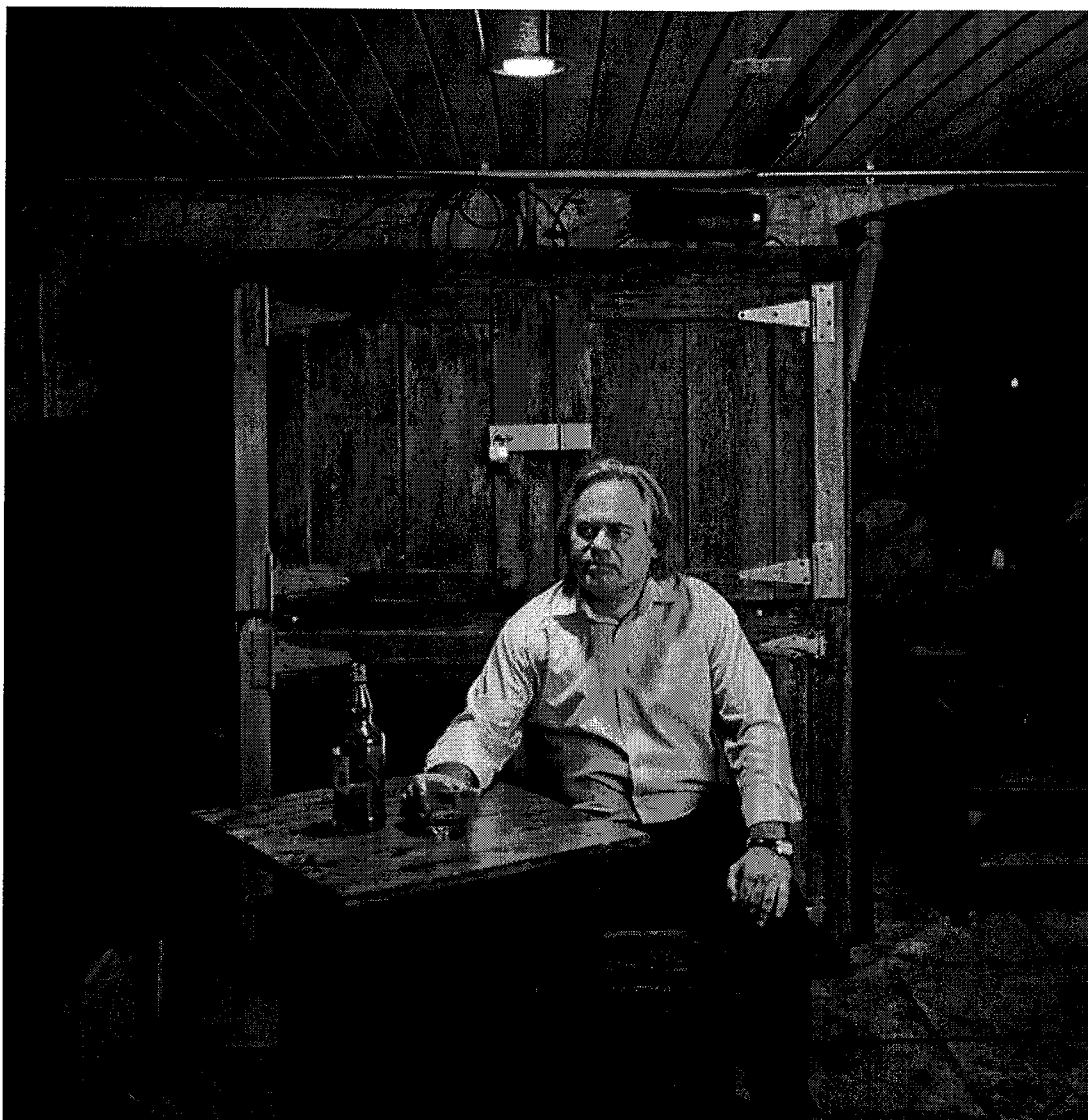
 RINGCENTRAL FAX
Business fax for desktops, smartphones and tablets
 RingCentral
[Free Trial](#)

NOAH SHACHTMAN MAGAZINE 07.23.12 4:00 AM

RUSSIA'S TOP CYBER SLEUTH FOILS US SPIES, HELPS KREMLIN PALS

Russia's Top Cyber Sleuth Foils US Spies, Helps Kre...

SUBSCRIBE



Eugene Kaspersky, Soviet officer turned software tycoon. Photo: Stephen Voss

SHARE

225

IT'S EARLY FEBRUARY in Cancun, Mexico. A group of 60 or so financial analysts, reporters, diplomats, and cybersecurity specialists shake off the previous night's tequila and file into a ballroom at the Ritz-Carlton hotel. At the front of the room, a giant screen shows a globe targeted by crosshairs. Cancun is in the center of the bull's-eye.

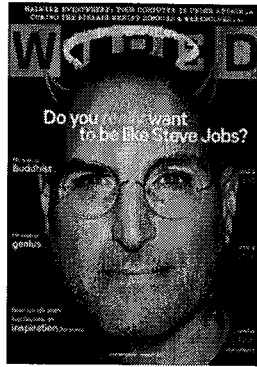
Also in this issue

- **Former McDonald's Honchos Take On Sustainable Cuisine**
- **Undead: The Rabies Virus Remains a Medical Mystery**
- **Will Wright Wants to Make a Game Out of Life Itself**

22

0

A ruddy-faced, unshaven man bounds onstage. Wearing a wrinkled white polo shirt with a pair of red sunglasses perched on his head, he looks more like a beach bum who's lost his way than a business executive. In fact, he's one of Russia's richest men—the CEO of what is arguably the most important Internet security company in the world. His name is Eugene Kaspersky, and he paid for almost



everyone in the audience to come here. “*Buenos dias,*” he says in a throaty Russian accent, as he apologizes for missing the previous night’s boozy activities. Over the past 72 hours, Kaspersky explains, he flew from Mexico to Germany and back to take part in another conference. “Kissinger, McCain, presidents, government ministers” were all there, he says. “I have panel. Left of me, minister of defense of Italy. Right of me, former head of CIA. I’m like, ‘Whoa, colleagues.’”

He’s bragging to be sure, but Kaspersky may be selling himself short. The Italian defense minister isn’t going to determine whether criminals or governments get their hands on your data. Kaspersky and his company, Kaspersky Lab, very well might. Between 2009 and 2010, according to *Forbes*, retail sales of Kaspersky antivirus software increased 177 percent, reaching almost 4.5 million a year—nearly as much as its rivals Symantec and McAfee combined. Worldwide, 50 million people are now members of the Kaspersky Security Network, sending data to the company’s Moscow headquarters every time they download an application to their desktop. Microsoft, Cisco, and Juniper Networks all embed Kaspersky code in their products—effectively giving the company 300 million users. When it comes to keeping computers free from infection, Kaspersky Lab is on its way to becoming an industry leader.

But this still doesn’t fully capture Kaspersky’s influence. Back in 2010, a researcher now working for Kaspersky discovered Stuxnet, the US-Israeli worm that wrecked nearly a thousand Iranian centrifuges and became the world’s first openly acknowledged cyberweapon. In May of this year, Kaspersky’s elite antihackers exposed a second weaponized computer program, which they dubbed Flame. It was subsequently revealed to be another US-Israeli operation aimed at Iran. In other words, Kaspersky Lab isn’t just an antivirus company; it’s also a leader in uncovering cyber-espionage.

Kaspersky has 300 million customers. His geek squad uncovers US cyberweapons. And he has deep ties to the KGB’s successors in Moscow.

Serving at the pinnacle of such an organization would be a remarkably powerful position for any man. But Kaspersky’s rise is particularly notable—and to some, downright troubling—given his KGB-sponsored training, his tenure as a Soviet intelligence officer, his alliance with Vladimir Putin’s regime, and his deep and ongoing relationship with Russia’s Federal

Security Service, or FSB. Of course, none of this history is ever mentioned in Cancun.

What is mentioned is Kaspersky's vision for the future of Internet security—which by Western standards can seem extreme. It includes requiring strictly monitored digital passports for some online activities and enabling government regulation of social networks to thwart protest movements. "It's too much freedom there," Kaspersky says, referring to sites like Facebook. "Freedom is good. But the bad guys—they can abuse this freedom to manipulate public opinion."

These are not exactly comforting words from a man who is responsible for the security of so many of our PCs, tablets, and smartphones. But that is the paradox of Eugene Kaspersky: a close associate of the autocratic Putin regime who is charged with safeguarding the data of millions of Americans; a supposedly-retired intelligence officer who is busy today revealing the covert activities of other nations; a vital presence in the open and free Internet who doesn't want us to be too free. It's an enigmatic profile that's on the rise as Kaspersky's influence grows.

Eugene Kaspersky was a bright kid.

At 16 he was accepted to a five-year program at the KGB-backed Institute of Cryptography, Telecommunications, and Computer Science. After graduating in 1987, he was commissioned as an intelligence officer in the Soviet army. A quarter century after the fact, he still won't disclose what he did in the military or what exactly he studied at the institute. "That was top-secret, so I don't remember," he says.



Eugene Kaspersky as a young Soviet military cadet.
Photo: courtesy Eugene Kaspersky

Kaspersky is more open about the day in October 1989 when a virus first infected his computer. It was a playful little thing called Cascade that made the characters on a PC screen tumble to the bottom like *Tetris* blocks. Curious, Kaspersky saved a copy of the virus on a floppy disk to study how the code worked. A couple of weeks later he encountered a second virus, and then a third. His interest grew with each discovery. "For Eugene, it was an addiction," his friend Alexey De Mont De Rique says. Each time a new virus appeared, Kaspersky would "sit in front of the computer for 20 hours straight," trying to pick it apart, De Mont De Rique recalls. In the small world of antivirus researchers, the Soviet officer quickly made a name for himself.

By the early '90s, Kaspersky wanted out of the army so he could study viruses

full-time. There was one small problem: "It was almost not possible," he explains. The only way to get out was to go to jail, get sick, or prove yourself to be extremely incompetent. Kaspersky's old instructor at the Institute of Cryptography had a company that sold everything from athletic shoes to PCs. Somehow—Kaspersky won't answer questions about this either—the former professor was able to get Kaspersky a discharge and hire him. Kaspersky's wife, Natalya, and De Mont De Rique soon joined him at the company.

In 1997 the three of them went into the antivirus business for themselves. Their software was advanced for the time. They were the first to allow users of Internet security software to watch malware operate in an isolated "sandbox," quarantined from the rest of the computer; they were among the first to store entire programs in a virus database. The young company flourished even as Kaspersky's marriage to Natalya fizzled. The couple divorced in 1998, but she continued to handle sales and finance while he worked in the "virus lab," classifying new threats himself. "The typical analyst would process maybe 100 pieces of new malware a day," says Aleks Gostev, one of Kaspersky's top researchers. "Eugene would do 300."

Today Kaspersky Lab employs about 200 virus researchers—some in the US and China, but the bulk of them in a converted electronics factory 6 miles northwest of the Kremlin. On a sunny April morning when I visit, the old factory feels more like a grad school, with tattooed twentysomethings from across the former Soviet Union roaming the curved halls. The school mascot seems to be Kaspersky himself. Some employees wear Che Guevara T-shirts—with the boss's face replacing the revolutionary's. On the walls are black-and-white photos of long-serving employees dressed in war paint and moccasins like Native Americans. "Eugene the Great Virus Hunter," reads the caption under the CEO's image—in which he's drawing a bow and arrow. Some 12,543 emails about suspicious programs came into the company just this morning, bringing the grand total to nearly 7.8 million.

'Rule number one of successful companies here is good relations with the secret police.'

The accumulation happens automatically. When a user installs Kaspersky software, it scans every application, file, and email on the computer for signs of malicious activity. If it finds a piece of known malware, it deletes it. If it encounters a suspicious program or a message it

doesn't recognize—and the user has opted to be part of the Kaspersky Security Network—it sends an encrypted sample of the virus to the company's servers. The cloud-based system automatically checks the code against a "whitelist" of 300 million software objects it knows to be trustworthy, as well as a "blacklist" of 94 million known malicious objects. If the code can't be found on either of these lists, the system analyzes the

program's behavior—looking at whether it's designed to make unauthorized changes to the computer's configuration options, for example, or whether it constantly pings a remote server. Only in the rare instance that the system is stumped will one of Kaspersky's T-shirt-clad virus researchers step in. They'll characterize the code by function: password stealer, bogus web page server, downloader of more malicious programs. Then they'll suggest a "signature" that can be used to spot and filter out the malware in the future. In just minutes, a software update that incorporates these new signatures can be pushed out to Kaspersky's tens of millions of users.

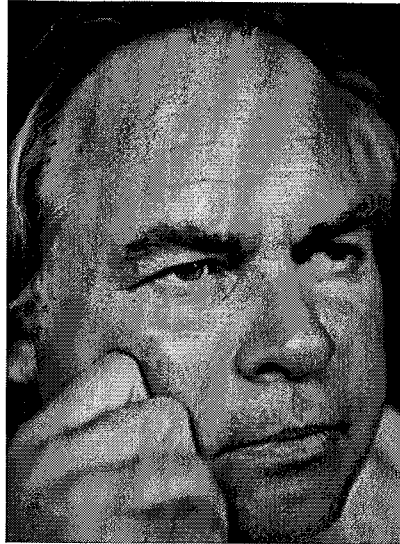
This is the core of the \$600-million-a-year business that grew out of Kaspersky's virus hobby. It's really not all that different from the way US security companies like Symantec or McAfee operate globally. Except for the fact that in Russia, high tech firms like Kaspersky Lab have to cooperate with the *siloviki*, the network of military, security, law enforcement, and KGB veterans at the core of the Putin regime.

The FSB, a successor to the KGB, is now in charge of Russia's information security, among many other things. It is the country's top fighter of cybercrime and also operates the government's massive electronic surveillance network. According to [federal law number 40-FZ \(.pdf\)](#), the FSB can not only compel any telecommunications business to install "extra hardware and software" to assist it in its operations, the agency can assign its own officers to work at a business. "Rule number one of successful companies here is good relations with the *siloviki*," says one prominent member of Russia's technology sector.

Kaspersky says the FSB has never made a request to tamper with his software, nor has it tried to install its agents in his company. But that doesn't mean Kaspersky and the security agency operate at arm's length. Quite the opposite: "A substantial part of his company is intimately involved with the FSB," the tech insider says. While the Russian government has used currency restrictions to cripple a firm's international business in the past, Kaspersky faces no such interference. "They give him carte blanche for his overseas operations, because he's among the so-called good companies."

Next door to the Moscow virus lab is the home base for another arm of the operation—a team of elite hackers from around the world that Kaspersky hand-selected to investigate new or unusual cybersecurity threats. Kaspersky calls this his Global Research and Expert Analysis Team—GREAT, for short. Two of them are waiting for me in their office. Sergei Golovanov sports rectangular glasses and a beard out of a '90s nu-metal video. Aleks Gostev is skinny as a rope and has dark circles under his eyes.

With Kaspersky's encouragement, GREAT has become increasingly active in helping big companies and law enforcement agencies track down cybercriminals. Gostev assisted Microsoft in its [takedown of the Kelihos botnet](#), which churned out 3.8 billion



Eugene Kaspersky's lab isn't just an antivirus company; it's also a leader in uncovering cyber-espionage.

Photo: Stephen Voss

pieces of spam every day at its peak. Golovanov spent months chasing the Koobface gang, which suckered social media users out of an estimated \$7 million.

One of GREAT's frequent partners in fighting cybercrime, however, is the FSB. Kaspersky staffers serve as an outsourced, unofficial geek squad to Russia's security service. They've trained FSB agents in digital forensic techniques, and they're sometimes asked to assist on important cases. That's what happened in 2007, when agents showed up at Kaspersky HQ with computers, DVDs, and hard drives they had seized from suspected crooks. "We had no sleep for a month,"

Golovanov says. Eventually two

Russian virus writers were arrested, and Nikolai Patrushev, then head of the FSB, emailed the team his thanks.

Kaspersky's public-sector work, however, goes well beyond Russia. In May, Gostev and Kaspersky were summoned to the Geneva headquarters of the International Telecommunication Union, the UN body charged with encouraging development of the Internet. The Russians were ushered into the office of ITU secretary-general Hamadoun Touré, where the Soviet-educated satellite engineer told them that a virus was erasing information on the computers of Iran's oil and gas ministry. This was coming just two years after the discovery of the Stuxnet worm, which had damaged Iran's centrifuges. Touré asked Kaspersky to look into it.

Back at the lab, analysts from GREAT began combing through archived reports from customers' machines. One file name stood out: ~DEB93D.tmp. The virus was eventually found on 417 customers' computers—398 of which were in the Middle East, including 185 in Iran. Some machines had been infected since 2010, but the file had never been deeply analyzed. The researchers were able to isolate one piece of the malicious code—and then another and another.

One module of the software surreptitiously turned on a machine's microphone and recorded any audio it captured. A second collected files, especially design and architectural drawings. A third uploaded captured data to anonymous command-and-control servers. A fourth module, with the file name Flame, infected other computers. The analysts discovered about 20 modules in all—an entire toolkit for online espionage. It was one of the biggest, most sophisticated pieces of spyware ever discovered. In honor of

the transmission program, the researchers called it Flame. On May 28, a Kaspersky analyst announced what the team had found.

Flame was another part of America's shadow war against Iran — and Kaspersky killed it.

The spyware was too complex for simple crooks or hacktivists, the researchers said. Flame had been coded by professionals, almost certainly at a government's behest. The company called it a cyberweapon and speculated that it was related to Stuxnet.

On June 1, *The New York Times* revealed for the first time that the White House had, in fact, ordered the deployment of Stuxnet as part of a sophisticated campaign of cyberespionage and sabotage against Tehran. Then, on June 19, *The Washington Post* was able to confirm that Flame was yet another part of this shadow war against Iran. Kaspersky had outed—and in effect killed—it.

For Kaspersky, exposing Flame reflects his company's broader ambition: to serve as a global crime-stopper and peacekeeper. Malware has evolved from a nuisance to a criminal tool to an instrument of the state, he says, so naturally he and his malware fighters have grown in stature and influence too. "My goal is not to earn money. Money is like oxygen: Good idea to have enough, but it's not the target," he says. "The target is to save the world."

In a locked room down the hall from his office, Kaspersky is working on a secret project to fulfill that lofty ambition. Not even his assistant has been allowed inside. But after we've spent a day together—and knocked back a few shots of Chivas 12—he unlocks the door and offers me a peek. It's an industrial control system, a computer for operating heavy machinery, just like the ones that Stuxnet attacked (and, Kaspersky researchers believe, Flame may also have targeted). Kaspersky's team is quietly working on new ways to harden these systems against cyberattack—to protect the power grids and prisons and sewage plants that rely on these controllers. The idea is to make future Stuxnets harder to pull off. The controllers haven't been engineered with security in mind, so the project is difficult. But if it succeeds, Kaspersky's seemingly outsize vision of his company's role in the world might become a little less outlandish.

In the meantime, there's always politics.



Kaspersky at the 2011 Brazilian Grand Prix, flanked by drivers from the Ferrari F1 team that he sponsors. Photo: courtesy of Kaspersky Lab

Kaspersky has cultivated the image of a wild man with cash to burn—the flamboyant say-anything, do-anything, drink-anything gazillionaire. In Asia, he’s clowned around in TV commercials with Jackie Chan. In Europe, Kaspersky sponsors the Ferrari Formula One team and goes on Dublin pub crawls with Bono. Back in Russia, he throws New Year’s parties for 1,500. The most recent one had a rock-and-roll theme; Kaspersky took the stage in a Harley jacket. Last summer he took some 30 people to Russia’s Kamchatka Peninsula for a volcano-hiking excursion. Then there are the Kaspersky Lab conferences disguised as boozy getaways (or perhaps vice versa): the “analysts’ summit” on Spain’s Costa del Sol, the “VIP executive forum” in Monte Carlo, the “press tour” in Cyprus, the whatever-it-was thing in Cancun.

All of this might lead some to dismiss Kaspersky as a dilettante plutocrat who drinks single-malt and gets made up for TV while his employees do the real technical work. But the critics would be missing the point: One of the systems Kaspersky is now trying to hack is politics, and his antics are part of the act. Every trip to Shanghai’s Formula One race or the London Conference on Cyberspace is another chance to court diplomats and politicians, another chance to extend his company’s influence. And one of his goals is to persuade policymakers to refashion the Internet into something more to his liking—and, as it happens, something more to the liking of the Putin government as well.

Kaspersky says it’s time to give up privacy online: ‘By protecting our right to freedom we actually

In one hotel ballroom after another, Kaspersky insists that malware like Stuxnet and Flame should be banned by international treaty, like sarin gas or weaponized anthrax. He argues that the Internet should be partitioned and

sacrifice it!

certain regions of it made accessible only to users who present an "Internet passport." That way, anonymous hackers wouldn't be able to get at sensitive sites—like, say, nuclear plants. Sure, it might seem like we'd be sacrificing some privacy online. But with all the advertisers, search engines, and governments tracking us today, Kaspersky argues, we don't really have any privacy left anyway. "You can have privacy if you live somewhere in the jungle or the middle of Siberia," he recently told a confab in the Bahamas.

The Internet grew from a network of researchers to the global nervous system in large part because practically anyone was able to access any part of it from anywhere—no ID needed. And the values of openness, freedom, and anonymity became deeply embedded in net culture and in the very architecture of the network itself. But to Kaspersky, these notions no longer work: By "protecting our right to freedom we actually sacrifice it! We sacrifice the right to safe Internet surfing and to not get infected by some nasty piece of malware at every step."

The idea of stripping some amount of privacy from the Internet is gaining traction in many sectors, thanks at least in small part to Kaspersky's lobbying. In Cancun, he was joined onstage by Alexander Ntoko, a top official at the International Telecommunication Union. "Why don't we have digital IDs as a de facto for everybody?" he asks. "When I'm going to my bank, I'm not going to cover my face." In other words, why should things be any different online?

The ITU was once a bureaucratic backwater. In recent years, however, the Russian and Chinese governments have been pushing to give the agency a central role in governing the Internet. Instead of the US-dominated nonprofits that currently coordinate domain names and promote technical standards, they want to turn authority over to a gathering of national governments represented by the ITU. It's a move that one of the Internet's creators, Vint Cerf, told Congress risks "losing the open and free Internet," because it would transfer power from geeks to government bureaucrats. The ITU is set to revisit the 24-year-old treaty governing international telecommunications in December.



Whether or not it secures this power, the ITU has found a willing ally in Kaspersky. When he traveled to ITU headquarters in Geneva, a few months

after Cancun, Kaspersky not only agreed to look into the attacks on the Iranian oil ministry, he also told ITU chief Touré that he would assign some of his top researchers to be on call to help the organization with any future investigations. It's a good deal for both men. Kaspersky gets to extend his influence—and maybe catch the next big cyberweapon. Touré and the ITU get a personal cybersecurity team.

But Kaspersky's closest political ties remain in Russia. As one of his country's most successful technology entrepreneurs—and, in many ways, Russia's spokesman for all things Internet—Kaspersky has hosted former president and current prime minister Dmitry Medvedev in his offices (see video below); Medvedev, in turn, appointed Kaspersky to serve in Russia's Public Chamber, which is charged with monitoring the parliament.

Kaspersky and the Moscow government have espoused strikingly similar views on cybersecurity. This goes beyond the security industry's basic mission of keeping data safe. When Kaspersky or Kremlin officials talk about responses to online threats, they're not just talking about restricting malicious data—they also want to restrict what they consider malicious *information*, including words and ideas that can spur unrest.

Kaspersky can't stand social networks like Facebook or its Russian competitor, VK (formerly known as VKontakte). "People can manipulate others with the fake information," he says, "and it's not possible to find who they are. It's a place for very dangerous action." Especially dangerous, he says, is the role of social networks in fueling protest movements from Tripoli to Moscow, where blogger Alexei Navalny has emerged as perhaps the most important dissident leader and sites like VK and LiveJournal have helped bring tens of thousands of people into the streets. Kaspersky sees these developments as part of a disinformation campaign by antigovernment forces to "manipulate crowds and change public opinion."

Nikolai Patrushev—the former FSB chief who now serves as Putin's top security adviser—makes a nearly identical case. In June he told a reporter that outside forces on the Internet are constantly creating tensions within Russian society. "Foreign sites are spreading political speculation, calls to unauthorized protests," he says.

Russia's government and its most famous technology entrepreneur have long had each other's backs, cooperating on cybercrime investigations and supporting each other's political agendas. But the two became utterly intertwined at 6:30 in the morning on April 19, 2011, when Kaspersky's cell phone rang in his London hotel room. According to the caller ID, it was Ivan, Kaspersky's 20-year-old son. But the voice on the other end was not Ivan. It was an older man who politely told Kaspersky: "We've got your son."



Eugene Kaspersky now travels in Russia with bodyguards, after the kidnapping of his son.
Photo: Stephen Voss

Outwardly, Kaspersky didn't react to the news of Ivan's kidnapping. He said he was tired and asked the caller to ring him back later in the morning—which the caller did, from another number. This time, Kaspersky said he was in an interview and told the guy to make a third call.

It was a ploy, a stall for time while Kaspersky hurriedly reached out to his corporate security manager, who reached out to the FSB. Ordinarily the Russian intelligence service isn't in the business of freeing kidnap victims. But Ivan Kaspersky wasn't your average abductee. "My first thought was that this is serious. Second, immediately call the FSB. And third, they are stupid to attack me," Kaspersky says. "I was 100 percent sure—well, 99 percent sure—that FSB and police would find them. We have very good relations with both the FSB cybersecurity department and the Moscow police department. They know us. They know us as people who support them when they need it. They started to work like crazy."

That night Kaspersky took the red-eye back to Moscow. He plodded his way through the morning rush hour, his phone ringing every few minutes. As the kidnapers made their demands—3 million euros in denominations of 500—they tried to cover their tracks, switching cell phones and SIM cards constantly. But with every call, the kidnapers were giving the FSB more data to track them down.

According to the caller ID, it was Kaspersky's kid. But the voice on the other end was

Kaspersky arrived at a police station in central Moscow and promptly passed out from anxiety and exhaustion. He and his ex-wife stayed there for the next four days, pacing the halls while

**an older man's, saying:
'We've got your son.'**

the FSB pored through call records and the Moscow cops staked out a suburban cabin where they believed Ivan was being held. After a few days,

the officers lured the kidnappers out of the house with the promise of a ransom payment. They were captured without a shot. Ivan was freed, a little grimy—there was no running water in the cabin—but otherwise fine. “It was probably the only period in his life when he was reading books,” jokes his mother, Natalya Kaspersky, who met him at the scene.

At first, Kaspersky publicly blamed himself for not adequately protecting his family. But later he started blaming something else: VK. Kaspersky said that the Russian social network had tempted Ivan into posting his address, phone number, even details of his internship at InfoWatch, Natalya's security company. “Social networks shouldn't encourage users to post that sort of information. If a site asks for private information, then criminal charges should be brought against it in the event of a leak,” Kaspersky told Russia's RT television channel in October. Widely viewed as a Kremlin propaganda outlet, RT aired the remarks as part of a documentary on the death of online privacy and the dangers of social networks, with Ivan's kidnapping as a primary example. The program encouraged people to protect themselves by dropping offline completely. As it happened, the documentary ran just as online opposition to the ruling party was starting to bubble up. In the months that followed, top bloggers and activists were detained by the government, and the FSB tried (unsuccessfully) to force VK to purge the pages of some groups from its network.

The Kaspersky kidnapping ended up being a tool for the ruling party. But according to Natalya, the whole kidnapped-because-of-VK story is nonsense. “They found him on social networks? It's not true. They followed him for a month or more. They knew all his ways, where he is going, whom he contacts,” she says. Yes, Ivan posted an address online—“a false address from an old house.” There's no way, she says, that this helped the kidnappers.

So why did Eugene Kaspersky publicly blame VK? Perhaps Kaspersky simply let his emotions get the better of him—his son had been kidnapped, after all. Perhaps he mistook the fake address Ivan posted for a real one. Whatever the reason, in the end, the son's kidnapping became a way to attack the father's political foes.

THE NEW YORKER
RADIO HOUR

Check your local stations for broadcast times.
Or subscribe to the podcast.

SPONSORED IN PART BY:
WNYC STUDIOS | audible | SQUARESPACE

https://www.wired.com/wp-content/uploads/archivehttp://www.youtube-nocookie.com/v/b3mtPqGUh2M?version=3&hl=en_US

Eugene Kaspersky now travels in Moscow with a team of bodyguards. He moved to a duplex in a gated community bordering a park—better for keeping his girlfriend and their infant son safe, he explains. A wraparound balcony overlooks the still-frozen Moskva River and the site of Kaspersky Lab’s new five-story headquarters. To the left you can almost see Kaspersky’s childhood home: a one-room shack originally built for prison laborers in the Stalin era.

It’s an early Sunday afternoon in late April. Kaspersky, smoking a Chinese cigarette, is wearing the same bargain-rack striped shirt he was wearing Friday. His mother, who also lives in the complex, heats up blintzes and opens some canned caviar. Up close it becomes clear that Kaspersky’s image as a mega-rich, hyperconnected playboy is mostly an act. In truth, he stays away from Russia’s oligarchs, whom he sees as little different from the cybercrooks he chases. He views his move into politics as a necessary evil, an offer he’s in no position to refuse. Kaspersky doesn’t bother with political rallies or Moscow’s famously immoderate nightlife; he’d rather be in an airplane seat on his way to some conference to share ideas with other technophiles. When he goes to places like Kamchatka, he says, he takes employees or clients. “I don’t have any friends outside of work.”

Sure, Kaspersky touts a Kremlin-friendly line. In Putin’s Russia, executives who don’t have a habit of disappearing.

While critics assume that Kaspersky’s company is a virtual arm of Russian intelligence, he and his staff insist, not unconvincingly, that their work with the FSB has its limits. They argue that using its software to spy on users would undermine the company’s credibility worldwide; it would be like the local locksmith moonlighting as a

cat burglar. That credibility is at the heart of Kaspersky Lab’s business. Without lots of customers, there would be no Kaspersky Security Network, no database of known threats or tally of infected machines.

Yes, Kaspersky publicly touts a Kremlin-friendly line. But in Putin’s Russia, executives who neglect to do so have a disturbing habit of winding up in jail or being forced into exile. Besides, you don’t need to be a Moscow crony to push against free speech and privacy online. Plenty of Western officials are doing that too. Until 2011, Italians had to present their ID cards before using Wi-Fi at an Internet café. The European Commission is now mulling a continent-wide system of “electronic authentication.” British prime minister David Cameron contemplated cracking down on social media after the 2011 London riots. And retired US vice admiral Mike McConnell wrote in *The Washington Post* about the “need to reengineer the Internet to make attribution ... more manageable.” He previously served as US director of

national intelligence—America’s top spy.

In many ways, the relationship between the Kremlin and Kaspersky Lab is the same as the one between Washington and the big US security companies. Moscow gives millions to Kaspersky to help secure government networks—much as the Pentagon pours millions into contracts with McAfee and Symantec. Kaspersky helps the FSB track down cybercrooks; McAfee and Symantec work with the FBI. Kaspersky employees brief the Duma, Russia’s parliament; American researchers brief Congress and the White House. These security firms have all become key players in their home countries’ network defenses and in cybersecurity investigations worldwide.

But while the American and Russian companies are similar, there are important differences. Stuxnet was a highly classified US operation serving one of the government’s top geopolitical goals. Symantec, a US company, went after it anyway. It’s hard to find a similar case of Kaspersky and the Kremlin working at cross-purposes.



In December 2011, Kaspersky came under criticism for appearing to do the opposite—ignoring an act of online criminality when it was politically convenient. On the eve of Russia’s parliamentary elections, massive denial-of-service attacks brought down social networks like LiveJournal, media outlets like Kommersant.ru, and the independent election watchdog Golos. It seemed to be a politically motivated hit on potential opponents and critics of the ruling regime. Yet Kaspersky Lab—which boasts that its software can spot and fight DDoS attacks—denied the existence of any such activity. “We detected none. Very strange,” Kaspersky tweeted. The next day he wrote on his blog that the attacks actually had been detected, but he speculated that many of the sites were victims of technical problems or perhaps their own popularity.

Kaspersky denies that he blew off the DDoS attacks in an attempt to curry favor with the ruling powers. (Then he claims that pro-Putin sites got hit by the online strikes as well.) But Andrei Soldatov, a muckraking investigative journalist whose Agentura.ru site was hammered in the attacks, has a very different view: “I cannot explain Kaspersky’s ignorance by anything but conscious intention to take the Kremlin’s side, a position very weird for the independent expert he claims to be.”

Kaspersky’s office has just the trappings you’d expect for someone who rose from a kid in a shack to become a continent-hopping mogul: a Ferrari racing

jacket, boxes of his software in Chinese and German, a model of *SpaceShipTwo*, the aircraft that's going to fly well-heeled tourists to the edge of the atmosphere (Kaspersky already has a \$200,000 ticket). Late one afternoon, he reaches into a small closet and pulls out a lab coat with his company's logo to show me. Behind that is a basketball jersey from the New Jersey Nets, the NBA team owned by Russian billionaire Mikhail Prokhorov. At the very back of the closet I glimpse the dark green dress jacket from Kaspersky's Soviet Army uniform. The garment is in pristine condition; it looks like it could still be worn in a military parade.

There are plenty of Russian magnates content to use their Kremlin connections and corruption-fueled profits to bully and buy their way into the global arena. Kaspersky has long tried to play a different game: He's an international entrepreneur and thinker who is from Putin's Russia, but not of it. Kaspersky's financial success and influence is a testament to how skillfully he has walked this fine line. Yet the questions endure: Can a company so valuable to Moscow's government ever be truly independent of it? And what else is hidden in the back of the closet, that the rest of the world can't see?

I go in for a closer look at the jacket. Kaspersky shuts the door. "It's nothing," he says, walking out of the room. "Let's find a drink."


#20.08 #CRAZY IVANS #CYBERSECURITY #EUGENE KASPERSKY #FLAME #INFO WAR #RUSSIA
#SPY VS. SPY #STUXNET

[VIEW COMMENTS](#)

SPONSORED STORIES POWERED BY OUTBRAIN

					
<p>THE CLAIMS GUYS Do You Know If You Had PPI? You Can Find Out For FREE*</p>	<p>VIRALMOZO 17 Times Cartoon Episodes Were Not For</p>	<p>VIR3 Should This Navy SEAL Grade Flashlight Be</p>	<p>VIRALMOZO The Most Stunning Plus Size Models - 15 Images</p>	<p>MREXTICS.COM Google Executive and his Wife Both Own this</p>	<p>INFOWAT 10 Optical Illusions That Are Completely Insane</p>

ROBOTICS
Check In

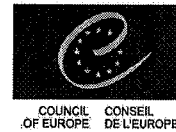


WE RECOMMEND

WIRED STAFF
The 10 Best Movies You Probably Didn't See in 2015



Exhibit L



Strasbourg, 24 February 2012

Opinion no. 661 / 2011

CDL-REF(2012)011
Engl. only

EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW
(VENICE COMMISSION)

FEDERAL LAW

ON THE FEDERAL SECURITY SERVICE¹

OF THE RUSSIAN FEDERATION

¹ Unofficial translation provided by the Council of Europe.

Translation from Russian

3 April 1995

No. 40-FZ

**RUSSIAN FEDERATION
FEDERAL LAW
ON THE FEDERAL SECURITY SERVICE**

Adopted
by the State Duma
on 22 February 1995

(as per Federal Laws No. 226-FZ of 30.12.1999,
No. 135-FZ of 07.11.2000, No. 49-FZ of 07.05.2002,
No. 116-FZ of 25.07.2002, No. 4-FZ of 10.01.2003,
No. 86-FZ of 30.06.2003, No. 122-FZ of 22.08.2004,
No. 15-FZ of 07.03.2005, No. 50-FZ of 15.04.2006,
No. 153-FZ of 27.07.2006, No. 124-FZ of 05.07.2007,
No. 211-FZ of 24.07.2007, No. 328-FZ of 04.12.2007,
No. 280-FZ of 25.12.2008, No. 238-FZ of 27.07.2010,
No. 275-FZ of 16.10.2010, No. 420-FZ of 28.12.2010,
No. 191-FZ of 11.07.2011, No. 241-FZ of 18.07.2011,
No. 424-FZ of 08.12.2011,

as amended by Federal Law No. 194-FZ of 30.12.2001)

The present Federal law defines the mission, composition, legal bases and principles of the activity of the Federal Security Service, the areas of activity, powers, manpower and resources of federal security service organs, and also the procedure for the monitoring and supervision of federal security service organs (preamble as per Federal Law No. 86-FZ of 30.06.2003)

**Chapter I.
GENERAL PROVISIONS**

Article 1. The Federal Security Service and its mission
(as per Federal Law No. 86-FZ of 30.06.2003)

The Federal Security Service is the unified central system of federal security service organs resolving tasks of safeguarding the security of the Russian Federation within the limits of its competence.

(as per Federal Law No. 15-FZ of 07.03.2005)

The activity of federal security service organs shall be directed by the President of the Russian Federation.

The Federal Security Service shall be administered by the head of the federal executive authority for security through the aforementioned federal executive authority and its territorial organs. The head of the federal executive authority for security shall be appointed and dismissed by the President of the Russian Federation.

Article 2. Federal security service organs

(as per Federal Law No. 86-FZ of 30.06.2003)

The organs of the Federal Security Service shall include:

the federal executive authority for security;

the directorates/departments of the federal executive authority for security covering the individual regions and constituent entities of the Russian Federation (territorial security organs);

the directorates/departments of the federal executive authority for security in the Armed Forces of the Russian Federation and other troop and military units and also their organs of administration (military security organs);

the directorates/departments/detachments of the federal executive authority for security for border service (border organs);
(as per Federal Law No. 15-FZ of 07.03.2005)

other directorates/departments of the federal executive authority for security exercising individual powers of that authority or carrying out federal security service authority activity (other security organs);
(as per Federal Law No. 15-FZ of 07.03.2005)

aviation sub-divisions, special training centres, special-purpose sub-divisions, enterprises,

education establishments, scientific research, expert, forensic, military medicine and military engineering sub-divisions and other establishments and sub-divisions assigned to carry out federal security service activity.

Territorial security organs, military security organs, border organs and other security organs are territorial organs of the federal executive authority for security and directly subordinate to it.

The federal executive authority for security, territorial security organs, military security organs and border organs may contain sub-divisions directly implementing main areas of activity of federal security service organs and administrative and support functions.
Fourth paragraph invalidated by Federal Law No. 15-FZ of 07.03.2005.

The creation of federal security service organs not provided for in the present federal law shall not be permitted.
(as per Federal Law No. 15-FZ of 07.03.2005)

Within federal security service organs the creation of structural sub-divisions of political parties and activity of political parties or public movements pursuing political aims and also the conducting of political agitation and pre-election campaigning shall be prohibited.
(as per Federal Law No. 15-FZ of 07.03.2005)

Article 3. Federal executive authority for security

(as per Federal Law No. 86-FZ of 30.06.2003)

The federal executive authority for security shall create its own territorial organs, organise the activity of those organs, issue regulatory acts within the limits of its competence and directly implement the main areas of activity of federal security service organs.
(as per Federal Law No. 15-FZ of 07.03.2005)

A Russian Federation Academy of Cryptography shall operate under the auspices of the federal executive authority for security. The statute of the Russian Federation Academy of Cryptography shall be ratified by the President of the Russian Federation.

Article 4. Legal basis for the activity of the Federal Security Service
(as per Federal Law No. 86-FZ of 30.06.2003)

The legal basis for the activity of the Federal Security Service shall comprise the Constitution of the Russian Federation, the present Federal law, other federal laws and other legal and regulatory acts of the Russian Federation.

The activity of the Federal Security Service shall also be carried out in accordance with the international treaties of the Russian Federation.

Article 5. Principles governing the activity of the Federal Security Service
(as per Federal Law No. 86-FZ of 30.06.2003)

The activity of the Federal Security Service shall be carried out on the basis of the following principles:

lawfulness;

respect for and observance of human and civil rights and freedoms;

humanism;

a unified system of federal security service organs and also centralisation of their administration;
(as per Federal Law No. 15-FZ of 07.03.2005)

secrecy, a combination of overt and covert methods and means of activity

Article 6. Observance of human and civil rights and freedoms in the activity of the Federal Security Service
(as per Federal Law No. 86-FZ of 30.06.2003)

The State shall guarantee observance of human and civil rights and freedoms in the implementation by the Federal Security Service of its activity. The restriction of human and civil rights and freedoms shall not be permitted except in cases provided for in federal constitutional laws and federal laws.

Any person believing that their rights and freedoms have been violated by federal security service organs or their officials shall be entitled to complain of the actions of those organs and officials to a higher authority of the Federal Security Service, a prosecutor's office or a court.
(as per Federal Law No. 15-FZ of 07.03.2005)

State authorities, enterprises, establishments and organisations, regardless of their form of ownership, and also public associations and citizens shall be entitled, in accordance with Russian Federation legislation, to obtain explanations and information from federal security service organs in the event of their rights and freedoms being restricted.
(as per Federal Law No. 15-FZ of 07.03.2005)

State authorities, enterprises, establishments and organisations, regardless of their form of ownership, and also public associations and citizens shall be entitled to demand compensation from federal security service organs for material and non-pecuniary damage caused by the actions of officials of said federal security service organs in the exercise of their official duties.
(as per Federal Law No. 15-FZ of 07.03.2005)

Information on the private life or impinging on the honour and dignity of a citizen or potentially harming their lawful interests which is obtained in the course of the activity of federal security service organs may not be communicated by federal security service organs to anyone whomsoever without the willing consent of the citizen concerned, except in cases provided for in federal laws.

(as per Federal Law No. 15-FZ of 07.03.2005)

In the event of a violation of human and civil rights and freedoms by federal security service organ staff, the head of the respective federal security service organ, a prosecutor or a judge shall be bound to take measures to restore those rights and freedoms, grant compensation for the damage caused and prosecute the perpetrators as provided for in Russian Federation legislation.

Federal security service organ officials misusing their authority or exceeding their official powers shall incur liability as provided for in Russian Federation legislation.

(as per Federal Law No. 15-FZ of 07.03.2005)

Article 7. Protection of Information on the Federal Security Service

(as per Federal Law No. 280-FZ of 25.12.2008)

Information on servicemen, federal state civil servants, federal security service organ workers, persons dismissed from federal security service organs, citizens engaged in military service under contract, federal state civil service or work in a federal security service organ, and persons assisting them or having assisted them on a confidential basis may be communicated by federal security service organs to other state authorities, other organisations and citizens only in the cases provided for in federal laws. In other cases the aforementioned information may be communicated on the basis of a decision of the head of the federal executive authority for security or an official authorised by them.

(first paragraph as per No. 241-FZ of 18.07.2011)

Physical individuals shall be granted access to information on federal security service organs constituting state secrets or other secrets protected by law under the procedure provided for in Russian Federation legislation on state secrets or other secrets protected by law, where there is no other provision in Russian Federation legislation.

Physical individuals may be refused access to information on federal security service organs constituting state secrets or other secrets protected by law on grounds provided for in Russian Federation legislation on state secrets or other secrets protected by law or for the sake of federal security service organs' own security.

Physical individuals may be permitted to participate in counter-intelligence activities, the combating of terrorism and crime, intelligence activities, border activities and information security activities carried out by federal security service organs (hereinafter - operational activities) and/or to access materials obtained as a result of carrying out such activity, under the procedure defined by the head of the federal executive authority for security.

Documents and materials containing information on servicemen, federal state civil servants, federal security service organ workers or persons assisting them or having assisted them on a confidential basis and also on the organisation, tactics, methods and means deployed by federal security service organs in carrying out operational activities shall be stored within federal security service organs.

Federal Security Service archive materials of historical or academic value and declassified in accordance with Russian Federation legislation shall be handed over for storage in the archives of the federal executive authority for archiving under the procedure established by Russian Federation legislation.

Article 7.1. Financial and material/technical support for Federal Security Service activity

(as per Federal Law No. 86-FZ of 30.06.2003)

The land and property of federal security service organs (including buildings, installations and equipment) created/being created or acquired/being acquired by means of federal budget resources or other resources shall be federal property.

(as per Federal Law No. 15-FZ of 07.03.2005)

Support for the activity of federal security service organs, including material/technical and financial support and creation of a support infrastructure shall be a mandatory expense for the Russian Federation.

(as per Federal Law No. 122-FZ of 22.08.2004 and No. 15-FZ of 07.03.2005)

Federal security service organs shall, on an unlicensed basis, devise, create, acquire and use arms and armaments, including special technical and other means, acquire and use military weaponry approved for the arming of federal security service organs by decision of the Russian Federation Government and also other service and non-military weaponry and the corresponding munitions.

(in the version of Federal Law No. 15-FZ of 07.03.2005)

The sale, transfer, exporting from the territory of the Russian Federation and importing onto the territory of the Russian Federation of arms and armaments, including special technical and other means, firearms and the corresponding munitions which may be used by federal security service organs, shall be carried out by federal security service organs under the procedure established by the Russian Federation Government.

(as per Federal Law No. 15-FZ of 07.03.2005)

The norms governing the supply of the basic arms issue types/systems/complexes and military and special equipment, the norms governing expenditure on motorised resources and fuel and also the procedure for service approval of arms, the acquisition, accounting, storage, issue, repair and decommissioning of arms issue types/systems/complexes and military and special equipment and the procedure for training federal security service organs in actions linked to the use of arms issue types/systems/complexes shall be established by the head of the federal executive authority for security in accordance with the Russian Federation Government-approved list of basic arms issue types/systems/complexes and military and special equipment and the procedure and norms for material and technical support for federal security service organs.

(as per Federal Law No. 15-FZ of 07.03.2005)

The building, reconstruction or granting for use of sites for the billeting of federal security service organs shall be carried out in accordance with the procedure and norms established by the Russian Federation Government for servicemen of the Armed Forces of the Russian Federation (with due regard to the special characteristics defined by the head of the federal executive authority for security), with funding from the federal budget and also funding from the organisations at whose initiatives the building or reconstruction of those sites is carried out.

(as per Federal Law No. 15-FZ of 07.03.2005)

Federal security service organs may possess service housing stock constituted under the procedure established by the Russian Federation Government.

(as per Federal Law No. 15-FZ of 07.03.2005)

Enterprises, establishments and organisations created or being created to support the activity of the Federal Security Service shall carry out their activities on an unlicensed basis and shall not be subject to privatisation.

Federal security service organs may, in accordance with Russian Federation legislation, requisition from federal executive authorities, executive authorities of Russian Federation constituent entities, local authorities, organisations, public associations and citizens of the Russian Federation means of transport and other property necessary for the fulfilment of the tasks assigned to those organs by federal legislation. The procedure for using the aforementioned property shall be defined by the head of the federal executive authority for security.

(as per Federal Law No. 15-FZ of 07.03.2005)

Tenth paragraph invalidated by Federal Law No. 122-FZ of 22.08.2004.

Land and natural resources shall be used by federal security service organs in accordance with federal legislation. Federal security service organs shall be exempt from all forms of payment for the use of natural resources.

(as per Federal Law No. 122-FZ of 22.08.2004 and No. 15-FZ of 07.03.2005)

Chapter II. MAIN AREAS OF ACTIVITY OF FEDERAL SECURITY SERVICE ORGANS

Article 8. Areas of activity of federal security service organs

(as per Federal Law No. 86-FZ of 30.06.2003)

The activity of federal security service organs shall be carried out in the following main areas:

counter-intelligence;
combating terrorism;
combating crime;
intelligence;
border activity;
safeguarding information security.

(first paragraph as per Federal Law No. 153-FZ of 27.07.2006)

Other areas of activity of federal security service organs shall be determined by federal legislation.

Article 9. Counter-intelligence

(as per Federal Law No. 153-FZ of 27.07.2006)

Counter-intelligence shall be an activity carried out by federal security service organs and/or their sub-divisions (hereinafter in the present Article "counter-intelligence organs"), as well as officials of those organs and sub-divisions by carrying out counter-intelligence measures for the purposes of detecting, preventing and suppressing intelligence-related and other activities of special services and organisations of foreign States, as well as of individuals seeking to harm the security of the Russian Federation.

Grounds for carrying out counter-intelligence measures by counter-intelligence organs shall be:

- a) the existence of information pointing to intelligence-related and other activities of special services and organisations of foreign States, as well as of individuals seeking to harm the security of the Russian Federation;
- b) [*б – in Russian*] the necessity of obtaining information on events or actions constituting a threat to the security of the Russian Federation;
- c) [*в – in Russian*] the necessity of ensuring the protection of information constituting state secrets;

d) [*z – in Russian*] the necessity of investigating/checking on individuals providing or having provided assistance to federal security service organs on a confidential basis;

e) [*o – in Russian*] the necessity of ensuring their own security;

f) [*e – in Russian*] requests made by special services, law enforcement agencies and other organisations of foreign States or by international organisations in accordance with the international treaties of the Russian Federation.

The list of grounds for carrying out counter-intelligence measures is exhaustive and may be amended or supplemented only by a federal law.

Counter-intelligence activity shall entail the carrying out of overt and covert measures, whose particular characteristics shall be defined by the special conditions in which that activity is carried out. The procedure for carrying out counter-intelligence measures shall be established by legal and regulatory acts of the federal executive authority for security.

The carrying out of counter-intelligence measures restricting the rights of citizens to secrecy of correspondence, telephone conversations, postal, telegraphic and other communications transmitted on electrical and telecommunications networks shall be permitted only on the grounds of a ruling by a judge and under the procedure provided for in Russian Federation legislation.

The carrying out of counter-intelligence measures restricting the right of citizens to the inviolability of their home shall be permitted only in the cases established by a federal law or on the grounds of a ruling by a judge.

In cases where it is necessary to carry out counter-intelligence measures restricting the constitutional rights of citizens mentioned in the present Article, the head of the counter-intelligence organ or their deputy shall lodge a corresponding application with a court. The decision to lodge the application shall set out the motives and grounds making it necessary to carry out the corresponding measures and the information corroborating the well-foundedness of the application (except for the information mentioned in the second paragraph of Article 24 of the present Law). A list of categories of heads of counter-intelligence organs and their deputies authorised to lodge an application to carry out counter-intelligence measures restricting the aforementioned constitutional rights of citizens shall be established by legal and regulatory acts of the federal executive authority for security.

Applications to carry out counter-intelligence measures restricting the aforementioned constitutional rights of citizens shall be examined without delay by a judge sitting alone who has jurisdiction for the location where such measures are to be carried out or for the location of the organ applying to carry them out.

After examining the application, the judge shall pronounce one of the following two rulings:

a) a ruling authorising the carrying out of counter-intelligence measures restricting the constitutional rights of citizens;

b) [*o – in Russian*] a ruling refusing the carrying out of counter-intelligence measures restricting the constitutional rights of citizens.

The period of validity of the ruling pronounced by the judge shall be calculated in days counted from the date on which it was pronounced and may not exceed 180 days, unless the judge takes another decision. In this case, the period of validity is not interrupted. Where it is necessary to prolong the period of validity of the ruling, the judge shall pronounce a ruling on the basis of newly submitted material.

A judge's refusal of the carrying out of counter-intelligence measures restricting the constitutional rights of citizens mentioned in the present Article may be appealed against by the applicant counter-intelligence organ to a higher court.

In urgent cases, where a delay may lead to the committing of a serious or particularly serious crime or where there is information on a threat to the state, military, economic or environmental security of the Russian Federation, on the basis of a reasoned decision of the head of the counter-intelligence organ or their deputy, the constitutional rights of citizens mentioned in the present Article may be restricted in the carrying out of counter-intelligence measures without a prior court ruling, with mandatory notification of the judge within 24 hours from the time when citizens' constitutional rights were restricted. The counter-intelligence organ shall be under obligation, within 48 hours from the time when citizens' constitutional rights were restricted, to obtain a judge's ruling authorising such restrictive action or discontinue its restrictive action.

The judge's ruling authorising the carrying out of counter-intelligence measures restricting the constitutional rights of citizens mentioned in the present Article and the materials serving as the basis for that ruling shall be stored in counter-intelligence organs.

The application by the head of a counter-intelligence organ or their deputy to carry out counter-intelligence measures restricting the constitutional rights of citizens mentioned in the present Article, the judge's ruling and the materials serving as a basis for that ruling shall be submitted to prosecution authorities in the event of checks being carried out under a supervisory procedure on materials, information and applications submitted by citizens claiming a violation of Russian Federation legislation by counter-intelligence organs.

The results of counter-intelligence measures may be used in criminal proceedings under the procedure established by criminal procedural legislation for using the results of operational/search activities.

Article 9.1. Combating terrorism

(paragraph 1 as per Federal Law No. 153-FZ of 27.07.2006)

Combating terrorism shall be an activity carried out by federal security service organs and/or their sub-divisions (hereinafter in the present Article "counter-terrorism organs"), as well as officials of those organs and sub-divisions for the purposes of detecting, preventing, suppressing, exposing and investigating acts of terrorism by carrying out special operations and other measures.

Grounds for carrying out counter-terrorism measures by counter- terrorism organs shall be:

- a) the necessity of suppressing a terrorist act;
- b) [*б – in Russian*] the necessity of identifying individuals involved in preparing or committing a terrorist act;
- c) [*в – in Russian*] the necessity of obtaining information on events or actions constituting a threat of terrorism.

Combating terrorism shall entail the carrying out of overt and covert special operations and other measures, whose special characteristics shall be defined by the conditions of combating of terrorism. The procedure for carrying out the aforementioned measures shall be established by legal and regulatory acts of the federal executive authority for security.

Counter-terrorism organs shall carry out their activities in accordance with legislation on operational/search activity, criminal and criminal procedural legislation, the present Federal law and other legal and regulatory acts of the Russian Federation.

The carrying out of counter-terrorism measures restricting the rights of citizens to the inviolability of their home and the secrecy of correspondence, telephone conversations, postal, telegraphic and other communications shall be permitted only on the grounds of a ruling by a judge obtained under the procedure established for the obtaining of a court decision on the admissibility of carrying out counter-intelligence measures restricting the rights of citizens to secrecy of correspondence, telephone conversations, postal, telegraphic and other communications transmitted on electrical and telecommunications networks and to the inviolability of their home and on the basis of a reasoned application by the head of a counter-terrorism organ or their deputy. A list of categories of heads of counter-terrorism organs and their deputies authorised to lodge an application to carry out counter-terrorism measures restricting the constitutional rights of citizens mentioned in the present Article shall be established by legal and regulatory acts of the federal executive authority for security.

The judge's ruling authorising the carrying out of counter-terrorism measures restricting the constitutional rights of citizens mentioned in the present Article and the materials serving as the basis for that ruling shall be stored in counter-terrorism organs.

In urgent cases, where a delay may lead to the committing of a terrorist act and endanger the lives and health of citizens, or where there is information from which it may be assumed that a terrorist act is being or has been committed on residential premises or in the pursuit of an individual suspected of involvement in committing a terrorist act, staff of a counter-terrorism organ shall be entitled to enter the residential premises unhindered and also to cut off the communications links of legal entities and physical individuals or to restrict the use of communication networks and means of communication. The counter-terrorism organ shall be under obligation to notify the prosecutor within 24 hours from the time when citizens' rights to the inviolability of their home were restricted or when the communications links of legal entities and physical individuals were cut off or the use of communication networks and means of communication were restricted.

The results of counter-terrorism measures may be used in criminal proceedings under the procedure established by criminal procedural legislation for using the results of operational/search activities.

The submitting of materials to prosecution authorities for the exercise of supervision by the prosecutor of the application of laws by counter-terrorism organs when carrying out counter-terrorism measures shall be governed by the provisions of Article 9 of the present Federal law.

Sub-divisions of special operations federal security service organs may be deployed, by decision of the President of the Russian Federation, against terrorists and/or their bases located outside the territory of the Russian Federation in order to eliminate a threat to the security of the Russian Federation.

Article 10. Combating crime

(as per Federal Law No. 86-FZ of 30.06.2003 and No. 153-FZ of 27.03.2006)

Federal security service organs shall carry out operational/search measures for the purposes of detecting, preventing, suppressing and exposing espionage, organised crime, corruption, illegal trading of arms and drugs and smuggling presenting a threat to the security of the Russian Federation and crimes whose investigation and preliminary examination are placed within their jurisdiction by law, and also for the purposes of detecting, preventing, suppressing and exposing the activities of illegal armed formations, criminal groups, individuals and public associations aiming to forcibly change the constitutional system of the Russian Federation.

(as per Federal Law No. 153-FZ of 27.07.2006)

Federal security service organs may be assigned other tasks in the sphere of combating crime by federal laws and other legal and regulatory acts of federal state authorities.

Federal security service organs shall carry out their activities in the sphere of combating crime in accordance with legislation on operational/search activity, criminal and criminal procedural legislation and the present Federal law.

(as per Federal Law No. 153-FZ of 27.07.2006)

Article 11. Intelligence activity

(as per Federal Law No. 86-FZ of 30.06.2003)

Intelligence activity shall be carried out by a foreign intelligence organ of the federal executive authority for security in accordance with the Federal Law "On foreign intelligence".

The procedure for cooperation between a foreign intelligence organ of the federal executive authority for security and other foreign intelligence organs of the Russian Federation shall be determined by federal legislation and agreements concluded between them on the basis thereof and/or joint legal and regulatory acts.

The procedure for carrying out intelligence measures and the procedure for using special methods and means in carrying out intelligence activity shall be determined by legal and regulatory acts of the federal executive authority for security.

Article 11.1. Border activity

(introduced by Federal Law No. 86-FZ of 30.06.2003)

Border activity shall be carried out in order to:

protect and preserve the state borders of the Russian Federation for the purpose of preventing unlawful changes to the lines of the state borders of the Russian Federation and ensure that physical individuals and legal entities respect the system of state borders of the Russian Federation, the frontier regime and the regime governing the points for crossing the state border of the Russian Federation;

protect and preserve the economic and other lawful interests of the Russian Federation within the boundaries of the border territory, exclusive economic zone and continental shelf of the Russian Federation, and also to preserve, beyond the boundaries of the exclusive economic zone of the Russian Federation, anadromous species of fish breeding in the rivers of Russia, transfrontier species of fish and species of fish migrating over larger distances in accordance with the international treaties of the Russian Federation and/or Russian Federation legislation.

(as per Federal Law No. 420-FZ of 28.12.2010)

Article 11.2. Safeguarding information security

(introduced by Federal Law No. 86-FZ of 30.06.2003)

Safeguarding information security shall be an activity carried out by federal security service organs within the limits of their competence:

in framing and implementing state and scientific/technical policy in the sphere of information security, including with the use of engineering/technical and cryptographic means;

in safeguarding through cryptographic and engineering/technical means the security of information and telecommunications systems, special communications networks and other communications networks for the transmission of encrypted information, in the Russian Federation and in the establishments thereof located outside the territory of the Russian Federation.

(as per Federal Law No. 424-FZ of 08.12.2011)

**Chapter III.
POWERS OF FEDERAL SECURITY SERVICE ORGANS**

Article 12. Duties of federal security service organs

Federal security service organs shall have a duty to:

- a) inform the President of the Russian Federation, the Chairman of the Russian Federation Government and, on their instructions, federal state authorities and also the state authorities of Russian Federation constituent entities of threats to the security of the Russian Federation;
- b) [*"б" in Russian*] detect, prevent and suppress intelligence and other activity of special services and organisations of foreign States, as well as of individuals seeking to harm the security of the Russian Federation;
- c) [*"в" in Russian*] obtain intelligence information in the interests of safeguarding the security of the Russian Federation and enhancing its economic, scientific/technical and defence capacity;
c.1) [*"в.1" in Russian*] carry out foreign intelligence activity in the sphere of encrypted, classified and other types of special communications from Russian Federation territory;
(*indent "c.1" ["в.1" in Russian] introduced by Federal Law No. 86-FZ of 30.06.2003*)
- d) [*"з" in Russian*] detect, prevent, suppress and expose crimes, whose investigation and preliminary examination are placed by Russian Federation legislation within the jurisdiction of federal security service organs, and also search for individuals having committed or suspected of committing the aforementioned crimes;
(*indent "д" ["з" in Russian] as per Federal Law No. 86-FZ of 30.06.2003*)
- d.1) [*"з.1" in Russian*] detect, prevent and suppress administrative infringements for which the initiation of proceedings and/or examination of cases are placed by the Russian Federation Code of Administrative Infringements within the jurisdiction of federal security service organs;
(*indent "d.1" ["з.1" in Russian] introduced by Federal Law No. 4-FZ of 10.01.2003*)
- e) [*"д" in Russian*] detect, prevent, suppress, expose and investigate terrorists which are being prepared or are being or have been committed, and also obtain information on events or actions constituting a threat of terrorism;
(*indent "е" ["д" in Russian] as per Federal Law No. 153-FZ of 27.07.2006*)
- f) [*"е" in Russian*] devise and implement, in collaboration with other state authorities, measures to combat corruption, illegal trade in arms and drugs, smuggling, activities of illegal armed formations, criminal groups, individuals and public associations aiming to forcibly change the constitutional system of the Russian Federation;
- g) [*"ж" in Russian*] safeguard within the limits of their competence security within the Armed Forces of the Russian Federation, other military forces, military formations and their administrative bodies, within organs in which military service is provided for by federal law and within internal affairs authorities, the State fire service, customs authorities and authorities controlling trade in drugs and psychotropic substances;
(*indent "г" ["ж" in Russian] as per Federal Law No. 86-FZ of 30.06.2003*)
- h) [*"з" in Russian*] safeguard within the limits of their competence the security of defence complex, nuclear power, transport and communications sites, life-sustaining facilities of cities and industrial centres and other strategic sites, and also security in the sphere of space research and priority scientific projects;
- i) [*"и" in Russian*] safeguard within the limits of their competence the security of federal state authorities and state authorities of Russian Federation constituent entities;

i.1) ["u.1" in Russian] organise and safeguard security in the sphere of encrypted, classified and other types of special communications in the Russian Federation and, within the limits of their competence, in establishments of the Russian Federation located outside its territory;
(indent "i.1" ["u.1" in Russian] introduced by Federal Law No. 86-FZ of 30.06.2003)

j) ["k" in Russian] participate in the devising and implementation of measures to protect information constituting state secrets; exercise supervision over the safekeeping of information constituting state secrets in state authorities, military formations, enterprises, establishments and organisations regardless of their form of ownership; take measures under the established procedure relating to citizens' access to information constituting state secrets;

k) ["n" in Russian] undertake measures in collaboration with the federal executive authority for foreign intelligence to safeguard the security of the Russian Federation's establishments and citizens outside its territory;
(as per Federal Law No. 86-FZ of 30.06.2003)

l) ["m" in Russian] take measures, within the limits of their competence, to protect and preserve the state borders of the Russian Federation and to protect and preserve the economic and other lawful interests of the Russian Federation within the boundaries of the border territory, exclusive economic zone and continental shelf of the Russian Federation, and also to exercise state control in the sphere of protecting marine biological resources, including the monitoring of vessels engaged in fishing in respect of transfrontier species of fish and species of fish migrating over larger distances in the open sea, in accordance with the international treaties of the Russian Federation and/or Russian Federation legislation.
(as per Federal Laws No. 86-FZ of 30.06.2003 and No. 420-FZ of 28.12.2010)

m) ["h" in Russian] safeguard, in collaboration with internal affairs authorities, the security of foreign States' representations in the Russian Federation;

n) ["o" in Russian] participate, within the limits of their competence and jointly with other state authorities, in the safeguarding of the security of public/political, religious and other mass events held on the territory of the Russian Federation;

o) ["n" in Russian] register and keep a centralised record of radio data and radio emissions produced by electronic radio transmitters; detect on the territory of the Russian Federation radio emissions produced by electronic radio transmitters whose operation poses a threat to the security of the Russian Federation, and also radio emissions produced by electronic radio transmitters used for illegal purposes;

p) ["p" in Russian] to participate, in accordance with Russian Federation legislation, in resolving matters pertaining to the conferring and renunciation of Russian Federation citizenship, entry to and exit from Russian Federation territory of Russian Federation citizens, foreign citizens and stateless persons, and also the procedure governing the residence of foreign citizens and stateless persons on Russian Federation territory;

q) ["c" in Russian] to maintain the mobilisation readiness of federal security service organs;

r) ["m" in Russian] to carry out vocational training.
(indent "r" ["m" in Russian] as per Federal Law No. 86-FZ of 30.06.2003)

Article 13. Rights of federal security service organs

Federal security service organs shall be entitled to:

a) establish on a confidential basis cooperation links with individuals consenting thereto;

a.1) use special methods and means in carrying out counter-intelligence and intelligence activity and also measures to combat terrorism;
(indent "a.1" introduced by Federal Law No. 86-FZ of 30.06.2003; as per Federal Law No. 153-FZ of 27.07.2006)

b) ["6 " in Russian] carry out operational/search measures to detect, prevent, suppress and expose espionage, organised crime, corruption, illegal trading of arms and drugs and smuggling presenting a threat to the security of the Russian Federation and crimes whose investigation and preliminary examination are placed by Russian Federation legislation within the jurisdiction of federal security service organs and also to detect, prevent, suppress and expose the activity of illegal armed formations, criminal groups, individuals and public associations aiming to forcibly change the constitutional system of the Russian Federation.
(as per Federal Law No. 153-FZ of 27.07.2006)

b.1) ["6.1 " in Russian] carry out special operations to suppress terrorist activity (special operations activity) and also create and use special methods and means to carry them out;
(indent "b.1" ["6.1 " in Russian] introduced by Federal Law No. 86-FZ of 30.06.2003)

b.2) ["6.2 " in Russian] use special-purpose sub-divisions of federal security service organs and deploy military equipment, arms and special means approved for the arming of federal security service organs and also physical force against terrorists and/or their bases located outside the territory of the Russian Federation in order to eliminate a threat to the security of the Russian Federation;

(indent "b.2" ["6.2 " in Russian] introduced by Federal Law No. 153-FZ of 27.07.2006)

c) ["8 " in Russian] infiltrate foreign States' special services and organisations carrying out intelligence and other activity aimed at damaging the security of the Russian Federation and also infiltrate criminal groups;

c.1) ["8.1 " in Russian] carry out foreign intelligence activity independently from the territory of the Russian Federation, and also in cooperation with other foreign intelligence organs of the Russian Federation and, on the basis of inter-state agreements, with special services and law enforcement agencies of foreign States in the sphere of encrypted, classified and other types of special communications using radio-electronic means and methods;

(indent "c.1" ["8.1 " in Russian] introduced by Federal Law No. 86-FZ of 30.06.2003)

d) ["2 " in Russian] conduct the investigation and preliminary examination of crimes placed by Russian Federation legislation within the jurisdiction of federal security service organs;

(as per Federal Law No. 50-FZ of 15.04.2006)

d.1) ["2.1 " in Russian] draw up reports on administrative infringements, pronounce decisions and rulings on cases of administrative infringements, fix administrative punishments for cases of administrative infringements, lodge requests to eliminate causes and conditions facilitating the committing of administrative infringements, and exercise other powers in cases of administrative infringements placed by the Russian Federation Code of Administrative infringements within the jurisdiction of federal security service organs;

(indent "d.1" ["2.1 " in Russian] introduced by Federal Law No. 4-FZ of 10.01.2003)

d.2) ["2.2 " in Russian] issue a physical individual with an official warning, with which they are bound to comply, of the inadmissibility of actions creating conditions for the committing of crimes for which investigation and preliminary examination are placed by Russian Federation legislation within the jurisdiction of federal security service organs, in the absence of grounds for criminal prosecution;

(indent "d.2" ["2.2 " in Russian] introduced by Federal Law No. 238-FZ of 27.07.2010)

e) ["0 " in Russian] carry out cipher work within federal security service organs and also to monitor compliance with secrecy rules in the handling of encrypted information by cipher sub-divisions of state authorities, enterprises, establishments and organisations irrespective of their form of ownership (except for Russian Federation establishments abroad);

f) ["e " in Russian] use for official purposes means of communications belonging to state enterprises, establishments and organisations and, in urgent cases, to non-state enterprises,

establishments and organisations and also public associations and citizens of the Russian Federation;

g) ["ж" in Russian] use in extremely pressing cases means of transport belonging to enterprises, establishments and organisations irrespective of their form of ownership or of public associations or citizens (except for means of transport which are exempted from such use by Russian Federation legislation) for the prevention of crimes, the pursuit and apprehending of persons who have committed or are suspected of having committed crimes, for the transportation of citizens in urgent need of medical assistance to medical establishments, and also for transportation to the scene of an incident. At the request of the owners of the means of transport concerned federal security service organs shall compensate them under the legally established procedure for the expenses or damage they have incurred as a result;

(as per Federal Law No. 226-FZ of 30.12.1999)

g.1) ["ж.1" in Russian] use, free of charge in the exercise of their duties, the waterways and airspace of the Russian Federation, the territory/water zones of airports, aerodromes/landing areas and sea and river ports regardless of their organisational and legal form and form of ownership, and also be provided, free of charge in the exercise of their duties, with flights and water transport;

(indent "g.1" ["ж.1" in Russian] introduced by Federal Law No. 86-FZ of 30.06.2003)

h) ["з" in Russian] enter without hindrance citizens' residential and other premises, plots of land belonging to them, the grounds and premises of enterprises, establishments and organisations irrespective of their form of ownership in the event of there being sufficient grounds to suppose that acts constituting a public danger is being or has been carried out there, whose detection, prevention, suppression, exposure and investigation have been placed by Russian Federation legislation within the jurisdiction of federal security service organs, and also in the event of pursuing persons suspected of committing such acts, if any delay may pose a threat to the lives and health of citizens. Federal security service organs shall notify the prosecutor within 24 hours of all such cases of entry into residential and other premises belonging to citizens;

(as per Federal Law No. 153-FZ of 27.07.2006)

h.1) ["з.1" in Russian] cordon off/block sectors/sites in order to suppress acts of terrorism or mass disturbances and also to search for persons having escaped from custody or pursue individuals suspected of committing crimes for which investigation and preliminary examination are placed by Russian Federation legislation within the jurisdiction of federal security service organs, inspecting means of transport where necessary. In that process, federal security service organs shall take steps to ensure the continuation of normal life-sustaining activity of the community and the functioning of the corresponding facilities for those purposes in that place;

(indent h.1) ["з.1" in Russian] introduced by Federal Law No. 226-FZ of 30.12.1999)

h.2) ["з.2" in Russian] temporarily restrict or prevent the movement of citizens and means of transport in an individual sector/at individual sites and oblige citizens to remain there or to leave that sector/site for the purposes of protecting the lives, health and property of citizens or carrying out urgent investigative activities or operational/search and counter-terrorism measures;

(indent h.2) ["з.2" in Russian] introduced by Federal Law No. 226-FZ of 30.12.1999)

i) ["у" in Russian] inspect citizens' and officials' identity documents where there are sufficient grounds to suspect them of committing a crime;

j) ["к" in Russian] conduct the administrative detention of persons having committed offences involving attempted or actual intrusion into the territory of special-regime sites under special guard, closed administrative-territorial formations and other sites under guard and also check their identity papers, obtain explanations from them, carry out personal searches on them and confiscate their possessions and documents;

k) ["л" in Russian] lodge with state authorities, administrations of enterprises, establishments and organisations, regardless of their form of ownership, and also with public organisations, a request, with which those bodies are bound to comply, to eliminate causes and conditions facilitating the carrying out of threats to the security of the Russian Federation and the committing of crimes for which investigation and preliminary examination are placed by Russian Federation legislation within the jurisdiction of federal security service organs;

l) ["м" in Russian] receive free of charge from state authorities, enterprises, establishments and organisations, regardless of their form of ownership, information required to perform the duties assigned to federal security service organs, except in cases where federal laws prohibit the communication of such information to federal security service organs;
(as per Federal Law No. 86-FZ of 30.06.2003)

m) ["н" in Russian] set up, under the procedure established by Russian Federation legislation, enterprises, establishments, organisations and sub-divisions required to perform the duties assigned to federal security service organs and support the activity of those organs;

n) ["о" in Russian] set up special-purpose sub-divisions to perform the duties assigned to federal security service organs;

o) ["п" in Russian] conduct forensic and other expert examinations and research;

p) ["р" in Russian] maintain external relations with special services and law-enforcement agencies of foreign States, exchange operational information and special technical and other means with them on a reciprocal basis within the limits of the competence of federal security service organs and in accordance with the procedure established by normative acts of the federal executive authority for security; conclude international treaties of the Russian Federation, under the established procedure and within the limits of their competence;
(as per Federal Law No. 86-FZ of 30.06.2003)

q) ["с" in Russian] send official representatives of federal security service organs to foreign States by agreement with special services or law-enforcement agencies of those States with a view to increasing the effectiveness of combating international crime;

r) ["м" in Russian] implement measures to safeguard their own security, including preventing foreign States' special services and organisations, criminal groups and individuals from using technical means to access information constituting state secrets which is protected by federal security service organs;

r.1) ["м.1" in Russian] independently select candidates (including on a competitive basis) for recruitment into military service under contract in federal security service organs from among Russian Federation citizens under the procedure defined by the head of the federal executive authority for security;

(indent r.1) ["м.1" in Russian] introduced by Federal Law No. 280-FZ of 25.12.2008)

s) ["у" in Russian] authorise the staff of federal security service organs to possess and carry standard-issue weapons and special means;

t) ["ф" in Russian] use the documentation of other ministries, departments, enterprises, establishments and organisations to conceal the identity of staff of federal security service organs and the departmental affiliation of their sub-divisions, premises and means of transport;

t.1) ["ф.1" in Russian] use, for urgent action to neutralise and prevent terrorist acts and violations of the Russian Federation state border system, means of transport belonging to them fitted with light and sound signal emitting devices and bearing special colour schemes on their outside surfaces;

(indent t.1) ["ф.1" in Russian] introduced by Federal Law No. 211-FZ of 24.07.2007, as per Federal Law No. 280-FZ of 25.12.2008)

- u) ["x" in Russian] conduct scientific research into problems of Russian Federation security;
- v) ["y" in Russian] assist enterprises, establishments and organisations, irrespective of their form of ownership, in the devising of measures to protect commercial secrets;
- w) ["z" in Russian] train officers on a paid basis or free of charge for foreign States' special services and the security services of enterprises, establishments and organisations, irrespective of their form of ownership, provided that this does not contravene the principles governing the activity of federal security service organs.
(as per Federal Law No. 86-FZ of 30.06.2003)
- x) ["w" in Russian] exercise, within the limits of their competence, regulation in the sphere of devising, producing, implementing and operating encryption/cryptographic means and telecommunications systems and complexes located on Russian Federation territory and protected by encryption means, and also in the sphere of the provision of information encryption services in the Russian Federation and detection of electronic devices for the covert obtaining of information, on premises and in technical installations;
(indent x.1) ["w.1" in Russian] introduced by Federal Law No. 86-FZ of 30.06.2003)
- y) ["u" in Russian] exercise state control over the organisation and functioning of cryptographic and engineering/technical security of information and telecommunications systems, special communications networks and other communications networks used to transmit information with the use of ciphers, monitor compliance with secrecy rules in the handling of encrypted information by cipher sub-divisions of state authorities and organisations on the territory of the Russian Federation and in its establishments abroad and also supervise, in accordance with their prerogatives, the protection of particularly important sites/premises and the technical facilities therein against the leakage of data through technical channels;
(indent y) ["u" in Russian] introduced by Federal Law No. 86-FZ of 30.06.2003, as per Federal Law No. 424-FZ of 08.12.2011)
- z) ["e" in Russian] participate in the defining of the procedure for devising, producing, implementing, operating and protecting technical means of processing, storing and transferring restricted information to be used in Russian Federation establishments abroad;
(indent z) ["e" in Russian] introduced by Federal Law No. 86-FZ of 30.06.2003)
- yu) ["o" in Russian] detect information interception devices on particularly important sites/premises and technical means for use in federal state authorities;
(indent yu) ["o" in Russian] introduced by Federal Law No. 86-FZ of 30.06.2003)
- ya) ["r" in Russian] obtain biological material and process genome information related to crimes for which investigation and preliminary examination are placed by Russian Federation legislation within the jurisdiction of federal security service organs;
(indent ya) ["r" in Russian] introduced by Federal Law No. 191-FZ of 11.07.2011)
- exercise other rights afforded to federal security service organs by federal legislation.
(second paragraph introduced by Federal Law No. 86-FZ of 30.06.2003)

Federal security service organs may not use the rights granted to them to perform duties not provided for in federal laws.

Article 13.1. Use of prevention measures by federal security service organs
(introduced by Federal Law No. 238-FZ of 27.07.2010)

The preventive measures used by federal security service organs shall include the lodging of requests to eliminate causes and conditions facilitating the carrying out of threats to the security of the Russian Federation and the issuing of official warnings of the inadmissibility of actions creating conditions for the committing of crimes for which investigation and preliminary

examination are placed by Russian Federation legislation within the jurisdiction of federal security service organs.

In the presence of sufficient elements uncovered in the operational activities of federal security service organs which point to causes and conditions facilitating the carrying out of threats to the security of the Russian Federation, the federal security service authorities shall lodge with the corresponding state authorities or administrations of enterprises, establishments and organisations, regardless of their form of ownership, and also with public organisations, a request, with which those bodies are bound to comply, to eliminate said causes and conditions facilitating the carrying out of threats to the security of the Russian Federation.

For the purpose of preventing the committing of crimes for which investigation and preliminary examination are placed by Russian Federation legislation within the jurisdiction of federal security service organs, in the presence of sufficient and previously confirmed information on acts of physical individuals creating conditions for the committing of the aforementioned crimes, and in the absence of grounds for their criminal prosecution, federal security service organs, having first informed the prosecutor thereof, may issue that individual with an official warning, with which they are bound to comply, of the inadmissibility of actions creating conditions for the committing of such crimes.

The head of the federal security service organ or their deputy who are empowered to issue an official warning of the inadmissibility of actions creating conditions for the committing of crimes for which investigation and preliminary examination are placed by Russian Federation legislation within the jurisdiction of federal security service organs, shall, within ten days after checking the information received on the committing of the aforementioned actions by a physical individual, take a decision as to whether to issue an official warning to that individual. Any such official warning shall be sent/handed to the physical individual concerned no later than five days from the date when that decision was taken.

(fourth paragraph as per Federal Law No. 275-FZ of 16.10.2010)

The procedure for lodging a request to eliminate causes and conditions facilitating the carrying out of threats to the security of the Russian Federation, the procedure for issuing an official warning of the inadmissibility of actions creating conditions for the committing of crimes for which investigation and preliminary examination are placed by Russian Federation legislation within the jurisdiction of federal security service organs, including the procedure for sending it/handing it over, the form of the official warning, and also the list of categories of heads of federal security service organs and their deputies empowered to lodge such requests or issue such official warnings shall be established by legal and regulatory acts of the federal executive authority for security.

A request to eliminate causes and conditions facilitating the carrying out of threats to the security of the Russian Federation or an official warning of the inadmissibility of actions creating conditions for the committing of crimes for which investigation and preliminary examination are placed by Russian Federation legislation within the jurisdiction of federal security service organs may be appealed against before a court and the authorities indicated in Article 6 of the present Federal Law.

Article 14. Use of arms, special means and physical force

(as per Federal Law No. 153-FZ of 27.07.2006)

The staff of federal security service organs shall be permitted to possess and carry standard-issue weapons and special means. They shall be entitled to use military equipment, arms, special means and physical force, including military combat tactics, in accordance with the legal and regulatory acts of the Russian Federation.

Article 15. Collaboration with Russian and foreign establishments

Federal security service organs shall carry out their activity in collaboration with federal state authorities, state authorities of Russian Federation constituent entities, enterprises, establishments and organisations, regardless of their form of ownership.

Federal security service organs may avail themselves of the possibilities afforded by other Russian Federation security forces under the procedure established by federal laws and the regulatory acts of the President of the Russian Federation.
(as per Federal Law No. 226-FZ of 30.12.1999)

State authorities and also enterprises, establishments and organisations shall be under obligation to assist federal security service organs in the execution of the duties assigned to them.

Physical persons and legal entities in the Russian Federation providing postal communications services and electronic communications services of all types, including scrambled, confidential, satellite communications systems, shall be under obligation, at the request of federal security service organs, to include in the apparatus additional hardware and software and create other conditions required by federal security service organs to implement operational/technical measures.

For the purposes of resolving the tasks of safeguarding the security of the Russian Federation, servicemen of federal security service organs may be seconded to state authorities, enterprises, establishments and organisations, irrespective of their form of ownership, with the consent of their heads and in accordance with the procedure established by the President of the Russian Federation, while remaining on military service.

Collaboration between federal security service organs and foreign States' special services, law-enforcement agencies and other organisations shall be established on the basis of international treaties of the Russian Federation.

**CHAPTER IV.
MANPOWER AND MEANS OF FSB ORGANS**

Article 16. Staff of federal security service organs

(as per Federal Law No. 280-FZ of 25.12.2008)

Federal security service organs shall be staffed (including on a competitive basis) by servicemen, federal state civil servants and workers (hereinafter - servicemen and civilian personnel). Federal security service organ servicemen performing service under contract and also federal state civil servants of federal security service organs and workers of federal security service organs assigned to service duties shall comprise the staff of federal security service organs.

A citizen of the Russian Federation who is not a citizen/subject of a foreign State and is able, by virtue of their personal, professional and psychological qualities, age, education and state of health to perform the duties assigned to them may be a member of staff of federal security service organs. The qualifications requirements in terms of education, work experience and professional knowledge and skills necessary to perform the duties of a member of staff of a federal security service organ shall be established by the head of the federal executive authority for security or an official authorised by them.

(as per Federal Law No. 241-FZ of 18.07.2011)

Russian Federation citizens may not be accepted for service or for work in federal security service organs and likewise servicemen and civilian staff of federal security service organs may be dismissed from service or from work on grounds provided for in Russian Federation legislation or in the event of them:

a) having a residence permit or other document confirming their right to permanent residence on the territory of a foreign State;

b) ["б" in Russian] refusing to undergo compulsory state fingerprint registration, the procedure for vetting and security clearance for information constituting state secrets, compulsory interview with the use of technical and other means which must not be harmful to life or health or cause damage to the environment, and compulsory testing for the use of drugs and psychotropic substances;

c) ["в" in Russian] having a current or past conviction, including a quashed or extinguished conviction, or if a criminal prosecution against them was dropped following the expiry of the statute of limitation or mediation between the parties or as a result of an act of amnesty or in connection with active repentance;

d) ["г" in Russian] failing to submit documents or information which must be submitted in accordance with legal and regulatory acts of the Russian Federation and legal and regulatory acts of the federal executive authority for security, or the submitting of falsified documents or knowingly false information;

e) ["д" in Russian] being a member of a political party or another public association pursuing political aims and/or participating in its activities.

(third paragraph introduced by Federal Law No. 241-FZ of 18.07.2011)

In the cases provided for in the third paragraph of the present Article, servicemen and civilian personnel of federal security service organs may be dismissed from service or from work in accordance with Russian Federation legislation.

(fourth paragraph introduced by Federal Law No. 241-FZ of 18.07.2011)

Servicemen and civilian staff of federal security service organs having registered ownership of property outside the frontiers of the Russian Federation shall be under obligation to take steps to alienate that property within the time limit determined by the head of the federal executive authority for security.

(fifth paragraph introduced by Federal Law No. 241-FZ of 18.07.2011)

The failure of a person to comply with one of the requirements regarding personal and professional qualities, age, education and state of health mentioned in the second paragraph of the present Article or other requirements established by the present Federal law shall be grounds for refusing them entry or transfer to military service under contract, federal state civil service or work in a federal security service organ and likewise for terminating their contract or labour agreement.

Information concerning the grounds for refusing entry to service or work in a federal security service organ shall be provided to the citizen in question with due regard for Russian Federation legislation regarding state secrets or other secrets protected by law.

Russian Federation citizens entering military service under contract, federal state civil service or work in a federal security service organ shall undergo vetting for the purposes of determining their suitability for service or work in federal security service organs, including by means of psychological testing under the procedure established by the head of the federal executive authority for security.

Russian Federation citizens who are highly qualified specialists and have reached the age of 40 years may be awarded their first military service contract, while those having reached the age limit for military service may receive a new military service contract under the procedure determined by the head of the federal executive authority for security.

Article 16.1. Service in federal security service organs
(introduced by Federal Law No. 280-FZ of 25.12.2008)

Staff of federal security service organs shall be guided in their service activities by federal laws and may not be bound by decisions of political parties, public associations and other organisations.

Servicemen of federal security service organs shall perform military service in accordance with Russian Federation legislation on the performance of military service with due regard to the special characteristics established by the present Federal law determining the specific nature of the duties carried out by them. When carrying out operational activities, staff of federal security service organs shall be subordinate only to their immediate and direct superior. Upon receiving an order or instruction contrary to federal law, a member of staff of a federal security service organ must be guided by federal law.

Staff of federal security service organs shall be under obligation in their service activity to comply with the code of ethics and service conduct of staff of federal security service organs ratified by the head of the federal executive authority for security. Staff of federal security service organs shall bear liability for any violation of the provisions of that code in accordance with Russian Federation legislation.
(third paragraph introduced by Federal Law No. 241-FZ of 18.07.2011)

The number of servicemen and civilian personnel of federal security service organs shall be determined by the President of the Russian Federation.

The powers of officials of federal security service organs to ratify service regulations, apply commendations and disciplinary punishment in respect of the serviceman subordinate to them and also award military ranks, appoint and dismiss servicemen (with the exception of servicemen holding the posts of top-ranking officers) shall be established by the head of the federal executive authority for security.

Military service contracts until the age of 65 years may be concluded with servicemen of federal security service organs who are highly qualified specialists and have reached the age limit for military service, under the procedure defined by the head of the federal executive authority for security.

Servicemen and civilian personnel of federal security service organs shall be prohibited from participating, in person or through persons authorised by them, in the administration of organisations (except for participation in the administration of a non-profit organisation on an unpaid basis, where this is required for the resolving of operational activity tasks, or participation in a general assembly of members of a non-profit organisation), from engaging in entrepreneurial activity and also from providing assistance to physical individuals and legal entities in carrying out such activity. Staff of federal security service organs shall be prohibited from combining military service in a federal security service organ/federal state civil service or work in a federal security service organ with other paid activity, other than academic, teaching or another creative activity, except in cases provided for in Russian Federation legislation and/or where it is required for the resolving of operational activity tasks.
(as per Federal Law No. 241-FZ of 18.07.2011)

Servicemen and civilian personnel of federal security service organs may receive decorations and honorary and other awards from political parties, public associations and other organisations under the procedure defined by the head of the federal executive authority for security.

Article 16.2. Measures for safeguarding federal security service organs' own security
(introduced by Federal Law No. 241-FZ of 18.07.2011)

Russian Federation citizens entering military service, federal state civil service or work in a federal security service organ and servicemen and civilian personnel of federal security service organs shall undergo:

a) psychological testing and testing for the use of drugs and psychotropic substances, testing for alcohol, drug or other toxic substance dependence, checks to establish their suitability for service or for work in federal security service organs and their compliance with the qualification requirements, including a compulsory interview with the use of technical and other means which must not be harmful to life or health or cause damage to the environment;

b) ["б" in Russian] a procedure of security clearance for information constituting state secrets;

c) ["в" in Russian] vetting linked to the safeguarding of the federal security service organ's own security, including with the use of technical and other means which must not be harmful to life or health or cause damage to the environment.

The examinations, testing and vetting referred to in the present Article shall be carried out in the cases, under the procedure and within the time limits determined by the head of the federal executive authority for security.

The consent of Russian Federation citizens entering military service, federal state civil service or work in a federal security service organ and servicemen and civilian personnel of federal security service organs to undergo the examinations, testing and vetting referred to in the present Article during their service or work shall be stipulated in their respective military service, civil service or work contract.

Servicemen and civilian personnel of federal security service organs shall be prohibited from publishing in media or on the Internet information and telecommunications network any information (including photographic, video and other materials) about themselves or other federal security service organ colleagues, making it possible to discover their departmental affiliation to federal security service organ personnel, their service activities and activities of federal security service organs, except in cases provided for in legal and regulatory acts of the Russian Federation and legal and regulatory acts of the federal executive authority for security.

Russian Federation citizens entering military service, federal state civil service or work in a federal security service organ and servicemen and civilian personnel of federal security service organs shall be under obligation to submit information to personnel units relating to the safeguarding of federal security service organs' own security, in accordance with the roster, the cases and procedure defined by the head of the federal executive authority for security.

Servicemen and civilian personnel of federal security service organs shall be permitted to establish contacts with foreign citizens under the procedure and in the conditions determined by the head of the federal executive authority for security.

Article 17. Legal protection of staff of federal security service organs

When carrying out their service duties, servicemen of federal security service organs shall be representatives of the federal state authorities and under the protection of the State. No-one, other than state authorities and officials empowered to do so by federal laws, may interfere with their service activities.

Hampering a member of staff of a federal security service organ in the carrying out of their service duties, insulting, resisting, committing violence or threatening violence against them in connection with the carrying out of their service duties shall incur the liability provided for in Russian Federation legislation.

The life and health, honour and dignity and also property of members of staff of a federal security service organ and of the members of their families shall be protected from criminal infringements in connection with the carrying out of their duties under the procedure provided for in Russian Federation legislation.

When carrying out their service duties, servicemen of federal security service organs may not be taken into custody, detained, subjected to a body search or have their possessions, private transport or transport used by them searched without a representative of federal security service organs being officially present or a court decision.

Information concerning staff of federal security service organs who have performed/are performing special missions in special services and organisations of foreign States or in criminal groups shall constitute a state secret and may be made public only with the written consent of the aforementioned staff and in the cases provided for in federal laws.

Article 18. Social Protection of staff of federal security service organs

(as per Federal Law No. 122-FZ of 22.08.2004)

The length of service accrued by servicemen in federal security service organs who are highly qualified specialists prior to their entering military service may be counted in their required period of service for the awarding of a pension and for the calculation of the percentage length-of-service coefficient in accordance with the procedure defined by the director of the federal executive authority for security.

(as per Federal Law No. 86-FZ of 30.06.2003)

The time served by staff of federal security service organs on special assignments in special services and organisations of foreign States or in criminal groups shall be calculated in length of service at a more favourable rate for the awarding of a pension, promotion and the calculation of the percentage length-of-service coefficient in accordance with the procedure defined by the Russian Federation Government.

Official salaries/wage rates of civilian personnel of federal security service organs shall carry a 25-percent supplement for work in federal security service organs.

(third paragraph as per Federal Law No. 49-FZ of 07.05.2002)

Fourth paragraph invalidated by Federal Law No. 49-FZ of 07.05.2002.

Servicemen of federal security service organs carrying out their service duties in rural locations shall be entitled to free travel on passing transport (except personal vehicles) upon production of their service pass.

(fourth paragraph as per Federal Law No. 122-FZ of 22.08.2004)

Servicemen of federal security service organs safeguarding the security of transport facilities shall be entitled to free travel on trains and river, sea and air craft within the boundaries of the facilities guarded without having to purchase tickets, solely while carrying out their service duties linked to the safeguarding of the security of transport facilities.
(fifth paragraph as per Federal Law No. 122-FZ of 22.08.2004)

Servicemen of federal security service organs using personal means of transport for service purposes shall receive monetary compensation under the procedure and of the amount established by the Russian Federation Government.

Servicemen of federal security service organs shall have telephones installed in their place of residence at the applicable rates within a period not exceeding one year from the date of their application.
(as per Federal Law No. 122-FZ of 22.08.2004)
Eighth and ninth paragraphs invalidated by Federal Law No. 122-FZ of 22.08.2004.

The time spent by servicemen of federal security service organs undergoing medical treatment in connection with injuries, contusions or maiming sustained in the carrying out of their official duties shall be unlimited, except where there is incontrovertible evidence demonstrating the possibility of them recovering their capacity for military service.
Eleventh paragraph invalidated by Federal Law No. 122-FZ of 22.08.2004.

Civilian personnel of federal security service organs and also their children up to eighteen years of age shall be entitled to medical assistance in military medical establishments and subdivisions of federal security service organs, covered by the federal budget funding allocated to the upkeep of federal security service organs.
(twelfth paragraph introduced by Federal Law No. 124-FZ of 05.07.2007)

Article 19. Persons assisting federal security service organs

Federal security service organs may recruit individuals with their consent to assist them in the performance of the duties assigned to federal security service organs on a public or covert/confidential basis, including as non-staff personnel. The powers of non-staff personnel of federal security service organs shall be defined by regulatory acts of the federal executive authority for security.
(as per Federal Law No. 86-FZ of 30.06.2003)

Persons assisting federal security service organs shall be entitled to:

- a) conclude a contract with federal security service organs on confidential cooperation;
- b) ["б" in Russian] receive explanations of their tasks, duties and rights from staff of federal security service organs;
- c) ["в" in Russian] use documents concealing their identity for secrecy purposes;
- d) ["з" in Russian] receive emoluments;
- e) ["д" in Russian] receive compensation for damage to their health or property sustained in the process of assisting federal security service organs.

Persons assisting federal security service organs shall be under obligation to:

- a) comply with the terms of the cooperation contract or agreement concluded with federal security service organs;

b) [*"б" in Russian*] carry out the instructions of federal security service organs for the implementation of the duties assigned to them;

c) [*"в" in Russian*] refrain from the deliberate provision of subjective, incomplete, false or defamatory information;

d) [*"г" in Russian*] not divulge information constituting a state secret and other information of which they become aware in the process of assisting federal security service organs.

The use of confidential assistance on a contractual basis from deputies, judges, prosecutors, lawyers, minors, clergymen and authorised representatives of officially registered religious organisations shall be prohibited.

Information on persons who assist or have assisted federal security service organs on a confidential basis shall constitute a state secret and may be made public only with the written consent of those persons and in the cases provided for in federal laws.

Article 20. Information Support for FSB Organs

For the purpose of carrying out their activities, federal security service organs may, on an unlicensed basis, devise, create and operate information systems, communications systems and data transmission systems, as well as means of protecting information, including cryptographic protection.

The presence in information systems of information on physical individuals and legal entities shall not be grounds for the taking of measures by federal security service organs restricting the rights of those individuals or entities.

The procedure for recording and using information on the committing of infringements with implications for the safeguarding of the security of the Russian Federation and also information on intelligence or other activity of foreign States' special services and organisations or individuals seeking to harm the security of the Russian Federation shall be established by regulatory acts of the federal executive authority for security.
(as per Federal Law No. 86-FZ of 30.06.2003)

Article 21 invalidated by Federal Law No. 86-FZ of 30.06.2003.

Article 22 invalidated by Federal Law No. 86-FZ of 30.06.2003.

Chapter V. MONITORING AND SUPERVISION OF THE ACTIVITY OF FEDERAL SECURITY SERVICE ORGANS

Article 23. Monitoring of the activity of federal security service organs

Monitoring of the activity of federal security service organs shall be exercised by the President of the Russian Federation, the Federal Assembly of the Russian Federation, the Russian Federation Government and judicial bodies within the limits of their competence, as defined by the Constitution of the Russian Federation, federal constitutional laws and federal laws.

Deputies/members of the Federation Council and deputies of the State Duma of the Federal Assembly of the Russian Federation shall be entitled in connection with the exercise of their parliamentary activities to obtain information on the activity of federal security service organs under the procedure defined by Russian Federation legislation.

Article 24. Supervision by the prosecutor

Supervision of the application of laws of the Russian Federation by federal security service organs shall be carried out by the Prosecutor General of the Russian Federation and prosecutors authorised by them.

Information on persons having provided or providing assistance to federal security service organs on a confidential basis and also on the organisation, tactics, methods and means used by federal security service organs to carry out their activity shall not fall within the scope of supervision by the prosecutor.

**Chapter VI.
FINAL PROVISIONS**

Article 25. Legal successors of federal security service organs

The Federal Security Service of the Russian Federation and the organs subordinate to it shall be the legal successors of the Federal Counter-Intelligence Service of the Russian Federation and its organs.

The servicemen and civilian personnel of counter-intelligence organs of the Russian Federation shall be considered to have performed military service or having worked in federal security service organs in the post they occupied without any recertification or reassignment and also without carrying out organisational staffing measures.

Article 26. Entry into force of the present Federal law

The present Federal law shall enter into force from the date of its official publication.

The Russian Federation Law "On federal state security service organs" (Official Gazette of the Congress of People's deputies of the Russian Federation and the Supreme Soviet of the Russian Federation, 1992, No. 32, art. 1871; 1993, No. 33, art. 1308; No. 36, art. 1438) shall be deemed invalid from the date of entry into force of the present Law.

It is hereby proposed to the President of the Russian Federation and the Russian Federation Government is hereby instructed to bring their legal and regulatory acts into line with the present Federal law.

President of the Russian Federation
B. Yeltsin

Moscow, Kremlin
3 April 1995
No. 40-FZ

APPENDIX

Federal Law no. 238-FZ of 27 July 2010

**"Amending the Federal Law
"On the Federal Security Service"
and the Code of Administrative Infringements
of the Russian Federation"**

Adopted by the State Duma on 16 July 2010

Ratified by the Federation Council on 19 July 2010

Article 1

Make the following amendments to Federal Law no. 40-FZ of 3 April 1995 "On the Federal Security Service" (Compendium of Legislation of the Russian Federation, 1995, no. 15, art. 1269; 2000, no. 1, art. 9; 2002, no. 30, art. 3033; 2003, no. 2, art. 156; no. 27, art. 2700; 2006, no. 17, art. 1779; no. 31, art. 3452; 2007, no. 31, art. 4008; 2008, no. 52, art. 6235):

1) supplement paragraph 1 of Article 13 with a sub-paragraph "d.2" [*"z.2" in the original Russian text*] worded as follows:

"d.2) [z.2] issue a physical individual with an official warning, with which they are bound to comply, of the inadmissibility of actions creating conditions for the committing of crimes for which detection and preliminary investigation is placed by Russian Federation legislation within the jurisdiction of the federal security service authorities, in the absence of grounds for criminal prosecution;"

2) Add an Article 13.1 worded as follows:

"Article 13.1. *Use of preventive measures by the federal security service authorities*
Preventive measures used by the federal security service authorities shall include the lodging of a request to eliminate causes and conditions facilitating the carrying out of threats to the security of the Russian Federation and the issuing of an official warning, with which compliance is mandatory, of the inadmissibility of actions creating conditions for the committing of crimes for which detection and preliminary investigation is placed by Russian Federation legislation within the jurisdiction of the federal security service authorities.

In the presence of sufficient elements uncovered in the operational activities of the federal security service authorities which point to causes and conditions facilitating the carrying out of threats to the security of the Russian Federation, the federal security service authorities shall lodge with the corresponding state authorities or administrations of enterprises, institutions and organisations, regardless of their form of ownership, and also with public organisations, a request, with which those bodies are bound to comply, to eliminate said causes and conditions facilitating the carrying out of threats to the security of the Russian Federation.

For the purpose of preventing the committing of crimes for which detection and preliminary investigation is placed by Russian Federation legislation within the jurisdiction of the federal security service authorities, in the presence of sufficient and previously confirmed information on acts of physical individuals creating conditions for the committing of the aforementioned crimes, and in the absence of grounds for their criminal prosecution, the federal security service authorities, having first informed the prosecutor thereof, may issue that individual with an official warning, with which they are bound to comply, of the inadmissibility of actions creating conditions for the committing of such crimes.

The head of the federal security service authority or their deputy who are empowered to issue an official warning of the inadmissibility of actions creating conditions for the committing of crimes for which detection and preliminary investigation is placed by Russian Federation legislation within the jurisdiction of the federal security service authorities, shall, within ten days following the receipt of information on the committing of the aforementioned actions by a physical individual, take a decision in the light of a check on that information as to whether to issue an official warning to that individual. Any such official warning shall be sent/handed to the physical individual concerned no later than five days from the date when that decision was taken.

The procedure for lodging a request to eliminate causes and conditions facilitating the carrying out of threats to the security of the Russian Federation, the procedure for issuing an official warning of the inadmissibility of actions creating conditions for the committing of crimes for which detection and preliminary investigation is placed by Russian Federation legislation within the jurisdiction of the federal security service authorities, including the procedure for sending it/handing it over, the form of the official warning, and also the list of categories of heads of federal security service authorities and their deputies empowered to lodge such requests or issue such official warnings shall be established by legal and regulatory acts of the Federal executive authority in the security sphere.

A request to eliminate causes and conditions facilitating the carrying out of threats to the security of the Russian Federation or an official warning of the inadmissibility of actions creating conditions for the committing of crimes for which detection and preliminary investigation is placed by Russian Federation legislation within the jurisdiction of the federal security service authorities may be appealed against before a court and the authorities indicated in Article 6 of the present Federal Law."

GARANT information system comment:

See review of amendments made by the present Federal Law to the Code of Administrative Infringements of the Russian Federation

Article 2

Make the following amendments to the Code of Administrative Infringements of the Russian Federation (Compendium of Legislation of the Russian Federation, 2002, no. 1, art. 1; no. 30, art. 3029; no. 44, art. 4295; 2003, no. 27, arts. 2700, 2708, 2717; no. 46, art. 4434; no. 50, arts. 4847, 4855; 2004, no. 31, art. 3229; no. 34, arts. 3529, 3533; 2005, no. 1, arts. 9, 13, 45; no. 10, art. 763; no. 13, arts. 1075, 1077; no. 19, art. 1752; no. 27, arts. 2719, 2721; no. 30, arts. 3104, 3131; no. 50, arts. 5247; 2006, no. 1, art. 10; no. 10, art. 1067; no. 12, art. 1234; no. 17, art. 1776; no. 18, art. 1907; no. 19, art. 2066; no. 23, art. 2380; no. 31, arts. 3420, 3438, 3452; no. 45, art. 4641; no. 50, art. 5279; no. 52, art. 5498; 2007, no. 1, arts. 21, 29; no. 16, art. 1825; no. 26, art. 3089; no. 30, art. 3755; no. 31, arts. 4007, 4008; no. 41, art. 4845; no. 43, art. 5084; no. 46, art. 5553; 2008, no. 18, art. 1941; no. 20, art. 2251; no. 30, art. 3604; no. 49, art. 5745; no. 52, arts. 6235, 6236; 2009, no. 7, art. 777; no. 23, art. 2759; no. 26, arts. 3120, 3122; no. 29, arts. 3597, 3642; no. 30, art. 3739; no. 48, arts. 5711, 5724; no. 52, art. 6412; 2010, no. 1, art. 1; no. 21, art. 2525; no. 23, art. 2790):

1) in Article 19.3:

a) supplement the title, after the words "psychotropic substances", with the words "an officer of the federal security service authorities,";

b) [6 – in Russian] add a paragraph 4 worded as follows:

"4. Failure to obey a lawful order or request given or made by an officer of the federal security service authorities in the performance of their duties and also hindering an officer in the performance of their duties

- shall be punishable by an administrative fine in the case of a citizen of between five hundred and one thousand roubles or administrative arrest for a period of up to fifteen days; or a fine of between one thousand and three thousand roubles in the case of an official; or a fine of between ten thousand and fifty thousand roubles in the case of a legal person."

c) [8 - in Russian] add an explanatory note worded as follows:

"Explanatory note. *The provisions of paragraph 4 of the present article shall not apply to citizens in the event of preventive measures being taken against them in accordance with the Federal Law "On the Federal Security Service".*

2) in paragraph 1 of Article 23.1, replace the words "paragraphs 1 and 3 of Article 19.3" with the words "paragraphs 1,3 and 4 of Article 19.3";

3) in sub-paragraph 56 of paragraph 2 of Article 28.3, after the words "Article 14.20," add the words "paragraph 4 of Article 19.3,".

President of the Russian Federation

D. Medvedev
Moscow, Kremlin
27 July 2010
no. 238-FZ

Exhibit M

2012-007612

LAW LIBRARY OF CONGRESS

RUSSIAN FEDERATION

TRANSLATION OF NATIONAL LEGISLATION INTO ENGLISH

Russian is the state language of the Russian Federation¹ and all federal legislation is adopted and published in Russian. (Official publication of laws is required by the Constitution.²) There is no official translation of Russian laws into foreign languages and existing translations are fragmented. These translations are offered by selected government agencies, international and nongovernment organizations, and individual publishers. Most of the existing online translations are offered by subscription databases, which make their translated texts available through LexisNexis and Westlaw. Except in the case of a few competent publishers, the quality of these translations is dubious.³

I. Official Publications

Russian federal laws, acts issued by the legislature, government regulations, presidential decrees, international treaties, and rulings of the Constitutional Court of the Russian Federation are published in two major sources that are designated as official publishers of Russian legislation:

- SOBRANIE ZAKONODATELSTVA ROSSIISKOI FEDERATSII [COLLECTION OF RUSSIAN FEDERATION LEGISLATION] (1994–), LC Call No. KLB7.R87.
- ROSSIISKAIA GAZETA [RUSSIAN NEWSPAPER] (1990–), LC Call No. not available, LC Control No. sn 91026628 (government-published daily newspaper, includes selected normative acts issued by federal executive agencies, rulings of the Supreme Courts, and some other acts).

Publications in the *Rossiiskaia Gazeta* are available online at <http://www.rg.ru>; however, it is not clear whether the online texts accessible through the newspaper's website are considered official. According to amendments to the Federal Law on Procedures for Publication and Entry into Force of Federal Constitutional Laws, Federal Laws, and Acts of the Federal Assembly of October 21, 2011, the government Internet portal of legal information at <http://www.pravo.gov.ru> is the official publisher of Russian legislation in electronic format.⁴

¹ KONSTITUTSIIA ROSSIISKOI FEDERATSII [CONSTITUTION OF THE RUSSIAN FEDERATION] [KONST. RF] art. 68.1.

² *Id.* art. 15.

³ BURNHAM WILLIAM ET AL., LAW AND LEGAL SYSTEM OF THE RUSSIAN FEDERATION 48 (2004).

⁴ SOBRANIE ZAKONODATELSTVA ROSSIISKOI FEDERATSII [SZ RF] 2011, No. 43, Item 5977.

II. Court Reporters

Rulings of the Russian Constitutional Court are published by two official sources mentioned above as well as in the Court's bulletin, and on the Court's website:

- KONSTITUTIONNYI SUD ROSSIISKOI FEDERATSII [CONSTITUTIONAL COURT OF THE RUSSIAN FEDERATION], <http://www.ksrf.ru>.

Rulings and major decisions of the other two highest courts, the Supreme Court of the Russian Federation and the Highest Court of Arbitration, are published in Russian in their respective court bulletins:

- BIULLETEN VERKHOVNOGO SUDA ROSSIISKOI FEDERATSII [BULLETIN OF THE RUSSIAN FEDERATION SUPREME COURT] (1992–), LC Call No. KLB18 .B58.
- VESTNIK VYSSHEGO ARBITRAZHNOGO SUDA ROSSIISKOI FEDERATSII [HERALD OF THE RUSSIAN FEDERATION HIGHEST COURT OF ARBITRATION] (1992–), LC Call No. KLB1829.A13 V47.

Decisions of lower courts are published on their websites.

III. Translations of Laws

A. Code Compilations

Major Russian laws are passed in the form of codes, which serve as a compilation of major provisions regulating a specific field of law. Selected codes have been translated into English and published as individual books. Civil and criminal codes are more likely to be translated than others:

- GRAZHDANSKII KODEKS ROSSIISKOI FEDERATSII: PARALLELNYYE RUSSKII I ANGLIISKII TEKSTY / CIVIL CODE OF THE RUSSIAN FEDERATION: PARALLEL RUSSIAN AND ENGLISH TEXTS (Peter B. Maggs & Alexei N. Zhiltsov eds., trans., Norma, Moscow, 2003), LC Call No. KLB494.31994 .A52 2003 GLOBAL.
- CIVIL CODE OF THE RUSSIAN FEDERATION: PARTS ONE, TWO, AND THREE (William E. Butler ed., trans., Oxford Univ. Press, Oxford/New York, 2002), LC Call No. KLB494.31994 .A52 2002.
- CRIMINAL CODE OF THE RUSSIAN FEDERATION (William E. Butler trans., Kluwer Law International, Boston, 3d ed. 1999), LOC Call No. KLB3794.31996 .A52 1999 GLOBAL.
- Sarah J. Reynolds, *Criminal Code of the Russian Federation*, in 39(4), 39(6) STATUTES AND DECISIONS: THE LAWS OF THE USSR AND ITS SUCCESSOR STATES, July–Aug., Nov.–Dec. 2003.

Translations of other codes, such as the Criminal Procedure Code, Criminal Correctional Code, Tax Code, Family Code, Labor Code, and Land Code, can be found in the collection of the Law Library of Congress.

B. Individual Laws

Translations of certain individual laws can be found in major publications on Russian law. For example, the Law on Activities of Attorneys and on Advokatura can be found here:

- WILLIAM E. BUTLER, *THE RUSSIAN LEGAL PRACTITIONER* (Eleven International Publishing, The Hague; International Specialized Book Services, Portland, 2011), LOC Call No. KLB1630 .B88 2011.

Similarly, major laws regulating corporate activities, copyright, and international relations are available in specific publications examining Russia's legal developments in individual areas. For instance, the Russian Federal Law on International Treaties of the Russian Federation can be found in English translation in the following source:

- WILLIAM E. BUTLER, *THE RUSSIAN LAW OF TREATIES* (Simmonds & Hill, London, 1997), LOC Call No. KLB2400.A31995 B88 1997 EAST.

Laws, government regulations, orders issued by individual ministerial offices, and international treaties related to exploration of natural resources can be found in English in the following periodical:

- *RUSSIA & NIS: BASIC OIL LAWS & CONTRACTS: ORIGINAL TEXTS* (Barrows, New York, 1993–), LOC Call No. KLA3366.A28 1993.

C. Comprehensive Collections

The most comprehensive collections of translations in all areas of Russian law include the following:

- WILLIAM E. BUTLER, *RUSSIA & THE REPUBLICS LEGAL MATERIALS* (Penn. State Univ., Juris Publishing, 2006–), LC Call No. KLA13 2006 GLOBAL. This publication is a regularly updated continuation of translations previously published by Columbia University.
- *STATUTES AND DECISIONS: THE LAWS OF THE USSR AND ITS SUCCESSOR STATES* (M.E. Sharpe, New York, 1991–), LC Call No. K23 .O9. This publication includes various acts that have become available for translation. Some issues include acts selected by relevance to the given topic.

IV. Translations of Court Decisions

Court judgments are usually not translated into English. Selected rulings of commercial courts are translated and published by major Russian commercial legal databases, such as Garant

(see section VI) and Kodeks. Some documents related to the judiciary, court practice, and selected rulings of the Supreme Court, including the historic 2003 decision on the application of international law principles by Russian regular courts, are published in English on the website of the Supreme Court of the Russian Federation:

- *English: Documents*, SUPREME COURT OF THE RUSSIAN FEDERATION, <http://www.supcourt.ru/catalog.php?c1=English&c2=Documents>.

V. Online Resources

Translations of Russian laws published online appear to be very fragmented. Most of the existing resources cover only one specific field of law. This is especially true for websites maintained by individual government ministries. A limited number of major documents related to a particular agency's jurisdiction can be found at the following sites:

- THE CENTRAL BANK OF THE RUSSIAN FEDERATION, <http://www.cbr.ru/eng>.
- CENTRAL ELECTION COMMISSION OF THE RUSSIAN FEDERATION, <http://cikrf.ru/eng/>.
- FEDERAL ANTIMONOPOLY SERVICE OF THE RUSSIAN FEDERATION, <http://en.fas.gov.ru/legislation/>.
- FEDERAL CUSTOMS SERVICE, <http://www.russian-customs.org/legislation/mlacts/index.html>.
- MINISTRY OF TAXATION OF THE RUSSIAN FEDERATION, <http://www.garweb.ru/project/mns/en/law/>.

Selected international organizations and companies maintain databases of national laws for the countries participating in these organizations or where a company is operating. Relevant sources for Russian law include the following:

- LEGISLATIONLINE.ORG, <http://www.legislationline.org/>. The Office for Democratic Institutions and Human Rights of the Organization for Security and Cooperation in Europe provides access to Russian laws on human rights issues, citizenship and immigration, elections, and law enforcement.
- *Competition Policy & Law Database*, ASIA-PACIFIC ECONOMIC COOPERATION (APEC), <http://www.apec.org.tw/doc/Russia.html#Competition>. The Russia section of this database offers a collection of Russian laws, regulations, and decisions on competition policies and consumer protection.
- *Intelligence Related Laws and Edicts*, FEDERATION OF AMERICAN SCIENTISTS, <http://www.fas.org/irp/world/russia/docs/index.html>, contains a collection of Russian laws on intelligence and antiterrorism activities. Unfortunately, most of these translations are outdated and do not reflect recent amendments.
- ERNST & YOUNG, <http://www.tax.eycis.info/>, provides a comprehensive database of translations that contains documents on tax and financial matters as well as general

normative acts. The database features current and previous versions of documents. Access to the database is free but requires registration.

Commercial legal databases offer a good, though not comprehensive, collection of translated texts. However, because these documents are not freely available, it is difficult to assess their quality in general:

- GARANT, <http://english.garant.ru/legislation/>, is a legal reference database that appears to be most commonly used in Russia. It claims to translate into English and publish about forty documents weekly.
- RUSSIANGOST, <http://www.russianguost.com>, is a database that advertises itself as the largest Russian online law library in English. According to its website, it contains over 20,000 translated regulatory documents.

Websites and private blogs maintained by individuals can also be used as a resource for locating translations of Russian laws:

- *Normative Acts of the RF in English*, YURIDICHESKII BLOG [LEGAL BLOG], <http://fin-lawyer.ru/2008/normativnye-pravovye-akty-rf-na-anglijskom-yazyke/>, appears to be a blog maintained by a private Russian attorney, and is the most diverse collection of links to websites containing free versions of translated Russian legal texts.
- USLUGI.RU, <http://jslugi.ru/legislationru>, is a Moscow law firm that provides its clients with translations of business laws.

Prepared by Peter Roudik
Director of Legal Research
March 2012

Exhibit N



Strasbourg, 20 June 2012

Opinion no. 661/2011

CDL-AD(2012)015
Or. Engl.

EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW
(VENICE COMMISSION)

OPINION

**ON THE FEDERAL LAW
ON THE FEDERAL SECURITY SERVICE (FSB)**

OF THE RUSSIAN FEDERATION

**Adopted by the Venice Commission
at its 91st Plenary Session
(Venice, 15-16 June 2012)**

On the basis of comments by

**Mr Iain CAMERON (Member, Sweden)
Mr Hubert HAENEL (Member, France)
Mr Jørgen Steen SØRENSEN (Member, Denmark)
Mr Anders FOGELKLOU (Expert, Sweden)**

TABLE OF CONTENT

I. Introduction3

 A. Preliminary remarks.....3

 B. Background information.....4

II. General standards relating to security services.....4

III. The FSB Law.....6

 A. Legal basis, activities and powers of FSB organs. Guarantees for the protection of fundamental rights6

 B. Monitoring and supervision of the FSB activities.....8

 C. FSB powers under the 2010 amendments - The preventive measures13

 a) Generally.....13

 b) Official warnings to physical persons14

 c) Requests to legal persons.....17

IV. Conclusions.....19

I. Introduction

1. By a letter of 19 December 2011, the Chair of the Monitoring Committee of the Council of Europe Parliamentary Assembly requested the opinion of the Venice Commission on the Federal Law of the Russian Federation on the Federal Security Service (CDL-REF(2012)011, hereinafter "the FSB Law").
2. The Opinion is based upon the assessment of the English translation of the consolidated version of the FSB law as provided to the Venice Commission by the Monitoring Committee as well as other relevant laws and decrees. The translations may not accurately reflect the originals.
3. Messrs Cameron, Haenel and Sorensen acted as rapporteurs. The present Opinion is based on their comments and those provided by Mr Fogelklou, expert, as well as on the information made available to the delegation of the Venice Commission during its visit to Moscow, on 9-10 February 2012 and at a meeting in Paris on 27 April 2012. The Commission wishes to express its appreciation to the Russian authorities for the information provided during the meeting in Paris.
4. The opinion was discussed at a meeting of the Sub-commission on Fundamental Rights on 15 March 2012. It was adopted by the Venice Commission at its 91st Plenary Session (Venice, 15-16 June 2012).

A. Preliminary remarks

5. The present Opinion is limited in scope and should not be seen as a comprehensive and detailed review of all the provisions of the FSB Law. As suggested by the Monitoring Committee in its request, its purpose was to provide an assessment of the most recent amendments to the Law, in particular those having extended the powers of FSB organs and officers through new instruments - the preventive measures - and to highlight any related issues of concern.
6. The Opinion therefore focuses on the amendments to the FSB Law, mainly Article 13 and the new Article 13.1 of the Law, adopted in July 2010. Nonetheless, since the analysis of the above-mentioned articles cannot disregard the more general context of the law, the Opinion also addresses other matters linked, at least indirectly, to the powers of the security service organs and, accordingly, contains suggestions relating to other provisions of the Law.
7. Caution is called for in drawing conclusions in this sensitive area. The Commission recalls what it has stated before, in its earlier Report on Democratic Oversight of the Security Services,¹ that security agencies tend to be governed by "unpublished rules and by classified policy decisions, which would not and could not be brought to the attention of the public or of the Commission. Deficient legal provisions might well have been corrected in practice or, vice-versa, good legal provisions might not be applied in the intended way in practice."

¹ CDL-AD(2007)016, adopted by the Venice Commission at its 71st Plenary Session (Venice, 1-2 June 2007), § 51.

B. Background information

8. In April 1995, the Russian Federation adopted a federal law "On Organs of the Federal Security Service in the Russian Federation"², defining the role, mission, structures and main responsibilities of the FSB, the principles governing its activities, as well as the FSB main resources and supervision mechanisms.

9. One of the prerequisites to the accession of the Russian Federation to the Council of Europe in February 1996 was to adapt the powers and structure of the FSB to a new legal and democratic framework, in line with the European values and applicable standards³. Since 1995, the Law has been amended on several occasions.

10. In 2010, as a response to the suicide bombing in Moscow metro in March of 2010, new amendments of the FSB Law were introduced⁴. Following these amendments (notably article 13.1) the FSB has the power to issue both *warnings* to individuals and *official requests* to organisations whose actions are deemed to be facilitating threats to the country's security or creating the conditions for crimes. According to the Russian authorities, these preventive measures are aimed at combating extremism and terrorism and at providing increased protection to Russian citizens in general.

11. At the earlier drafting stage, the 2010 amendments were subject to public analysis and comment, both in Russia and internationally. In particular, this initiative was received with strong criticism by the Russian civil society and most of its representative organisations. According to the latter, the new provisions give the FSB back the powers of special services of totalitarian regimes and allow to stifle dissent and to scare political activists away from holding protests and rallies. One could indeed recall that the predecessor of the FSB, the KGB, working in a completely different political and legal climate in 1970's and in the beginning of the 1980's, had preventive measures as one of its main instrument. The criticism led to certain amendments being made, and the final text differs from the earlier draft (administrative penalties for non-compliance with the warnings were removed: see below, para. 54).

12. Further amendments to certain provisions of the FSB Law, on issues relating to the protection of information on the FSB (article 7), the FSB staff (article 16), service in FSB organs (article 16.1) and the FSB organs' own security (article 16.2) were adopted in July and December 2011.

II. General standards relating to security services

13. All provisions relating to the missions and prerogatives of national security services concern, in essence, the relationship between, on the one hand, the preservation of the interests of the nation and, on the other hand, the guarantees of fundamental rights and freedoms of citizens.

14. The human rights obligations of relevance in the analysis of the FSB law flow principally from the European and international standards as defined in the Universal Declaration of

² Russian Federation Federal Law No. 40-FZ of 3 April 1995.

³ "10. The Parliamentary Assembly notes that the Russian Federation shares fully its understanding and interpretation of commitments entered into as spelt out in paragraph 7, and intends: [...] xvii. to revise the law on federal security services in order to bring it into line with Council of Europe principles and standards within one year from the time of accession: in particular, the right of the Federal Security Service (FSB) to possess and run pre-trial detention centres should be withdrawn;" (See Parliamentary Assembly, *Opinion No. 193 (1996)1 on Russia's request for membership of the Council of Europe*).

⁴ Federal Law No. 238-FZ of 27 July 2010 "amending the Federal Law on the Federal Security Service and the Code of Administrative Infringements of the Russian Federation" and Federal Law No. 275-FZ of 16 October 2010.

Human Rights of 10 December 1948, the International Covenant on Civil and Political Rights of 16 December 1966 (ICCPR) and in particular the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) of 4 November 1950, with its Protocols. Further international instruments, such as the Council of Europe Convention on the Prevention of Terrorism (CETS No. 196) and the Shanghai Convention on Combating Terrorism, Separatism and Extremism⁵ are of relevance in this analysis.

15. The main ECHR relevant rights are the right to respect for private and family life (Article 8), the freedom of thought, conscience and religion (Article 9), the freedom of expression (Article 10) and freedom of assembly and association (Article 11), as well as the right to a fair trial (Article 6). The FSB Law has to be examined in the light of the permitted restrictions of the above-mentioned rights and freedoms. The Venice Commission recalls that the restriction clauses under the ECHR require for any limitation to the exercise of these a legal basis, a legitimate aim and to be "necessary in a democratic society", i.e. according to the long established jurisprudence of the ECtHR to correspond to a pressing social need, be proportionate and be relevant and sufficient.

16. In its *Guidelines on Human Rights and the Fight against Terrorism*, adopted on 11 July 2002, the Committee of Ministers of the Council of Europe indeed underlines the "States' obligation to respect, in their fight against terrorism, the international instruments for the protection of human rights and, for the member states in particular, the Convention for the Protection of Human Rights and Fundamental Freedoms and the case-law of the European Court of Human Rights"⁶.

17. At the same time, in its Recommendation 1713 (2005), adopted in the wake of the events of 11 September 2001, the Parliamentary Assembly of Council of Europe stressed the fundamental importance of the "democratic control of security sector". The recommendation of the Assembly is that the operation of security services must be based on clear and appropriate legislation, supervised by the judiciary, with parliamentary information. Moreover, the use of exceptional procedures must be defined by law in precise limits of time.

Previous Venice Commission reports

18. The Commission adopted an early report on internal security services in Europe on 7 March 1998.⁷

19. More recently, the Venice Commission has addressed in detail the challenges faced by states in the efforts aimed at the preservation of their internal and external security, with a particular focus on the accountability and the democratic supervision of security agencies, in the already mentioned *Report on the Democratic Oversight of the Security Services*.⁸ The best practices identified in this report as a whole should be of interest to the Russian Federation

⁵ Shanghai Convention on Combating Terrorism, Separatism and Extremism, 15 June 2001, available at: <http://www.unhcr.org/refworld/docid/49f5d9f92.html>

⁶ At the UN level, see in particular Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin: Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight, A/HRC/14/46 General Assembly, 17 May 2010.

<http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.46.pdf>

⁷ Venice Commission, *Report on Internal security services in Europe*, CDL-INF (1998)006, 7 March 1998, [http://www.venice.coe.int/docs/1998/CDL-INF\(1998\)006-e.pdf](http://www.venice.coe.int/docs/1998/CDL-INF(1998)006-e.pdf)

⁸ CDL-AD(2007)016. See also *Opinion of the Venice Commission on PACE Recommendation 1713(2005) on Democratic Oversight of the Security Sector in Member States*, CDL-AD(2005)033 and its *Opinion on the law on the information and security service of the Republic of Moldova*, CDL-AD(2006)011.

(and to any other state which wishes to improve oversight). For reasons of space, the present report will only cite the recommendations made and best practices identified which are of most relevance to the Russian Federation.

20. The Commission has also touched upon a number of these issues in its reports on counter-terrorism measures and human rights, adopted in July 2010⁹ on Private Military and Security Firms and Erosion of the State Monopoly on the use of force¹⁰, as well as in its opinions on Video Surveillance by Private Operators in the Public and Private Spheres and by Public Authorities in the Private Sphere and Human Rights Protection¹¹; on Video Surveillance in Public Places by Public Authorities and the Protection of Human Rights¹²; on the International legal obligations of Council of Europe member States in respect of secret detention facilities and inter-state transport of prisoners¹³.

III. The FSB Law

A. Legal basis, activities and powers of FSB organs. Guarantees for the protection of fundamental rights

21. The Law describes the FSB as the unified central system of federal security service organs in charge of the tasks of safeguarding, within the limits of its competence, the security of the Russian Federation. As stipulated by article 1 of the Law, its activities are directed by the President of the Russian Federation. The Law also indicates that the FSB operates as a federal executive authority (with its territorial organs)¹⁴ and that its head is appointed and dismissed by the President of the Russian Federation. The FSB is divided into various administrative and regional levels etc. as prescribed by article 2 of the Law.

22. The main areas of activity of FSB organs are defined (articles 8-11) as "counter intelligence", "combating terrorism", "combating crime", "intelligence", "border activity" and "safeguarding information security".

23. The legal basis governing the activities and operations of the FSB is specified in article 4 of the Law and includes: the Russian Federation Constitution, the 1995 Law, other federal laws and other legal and regulatory acts of the Russian Federation. In addition, FSB activities must be carried out "in accordance with the international treaties" to which the Russian Federation is a party.

⁹ CDL-AD(2010)022, *Report on Counter-terrorism Measures and Human Rights adopted by the Venice Commission at its 83rd Plenary Session (Venice, 4 June 2010)*

¹⁰ CDL-AD(2009)038, *Report on Private Military and Security Firms and Erosion of the State Monopoly on the use of force, adopted by the Venice Commission at its 79th Plenary Session (Venice, 12-13 June 2009)*.

¹¹ CDL-AD(2007)027, *Opinion on video surveillance by private operators in the public and private spheres and by public authorities in the private sphere and human rights protection, adopted by the Venice Commission at its 71st Plenary Session (Venice, 1-2 June 2007)*.

¹² CDL-AD(2007)014, *Opinion on Video Surveillance in Public Places by Public Authorities and the Protection of Human Rights, adopted by the Venice Commission at its 70th Plenary Session (Venice, 16-17 March 2007)*.

¹³ CDL-AD(2006)009, *Opinion on the International legal obligations of Council of Europe member States in respect of secret detention facilities and inter-state transport of prisoners adopted by the Venice Commission at its 66th Plenary Session (17-18 March 2006)*.

¹⁴ In its *Report on Internal Security Services in Europe*, the Venice Commission already had occasion to point out that security services can be conceived "... as an autonomous body and a separate organ or as part of the Executive directly responsible to a Minister or appropriate committee. In any case, however, the internal security services must be made accountable for their actions within the provisions of the law that regulates them." (CDL-INF(1998)006, conclusion (b)).

24. According to article 5 of the Law, FSB activities are based on the principles of lawfulness; respect for and observance of human and civil rights and freedoms; humanism; a "unified system of federal security service organs and also centralization of their administration", as well as "secrecy, a combination of overt and covert methods and means of activity".

25. Article 10¹⁵ refers to the competence of the FSB to engage in operational/search measures in relation to crimes within FSB jurisdiction. These are set out in another law, namely Article 151 of the Code of Criminal Procedure, which refers to sixty three crimes.

26. High degree of clarity of the law is necessary for an instrument governing the legal framework applicable to the security service.¹⁶

27. The protection and respect of fundamental rights represents an essential condition for the operation of security services as part of a democratic society and requires solid and specific guarantees. The Venice Commission therefore welcomes the inclusion of a specific provision in the Law (article 6), which requires the State to ensure respect for human rights in the action of the security service organs¹⁷. Article 4, as already mentioned, refers to compliance with international treaties, and this naturally includes the ECHR. Moreover, under Article 15 of the Constitution, treaties have primacy over laws and under Article 55 § 3 of the Constitution "Rights and freedoms of individual and citizen may be restricted by federal law only to the extent needed for the purposes of protecting the foundations of its constitutional system, morals, health, rights and legitimate interests of other persons, and ensuring the defence of the nation and security of the state". Having said this, no specific mention is made in the law on the FSB of the conditions applicable, under the ECHR, to any limitations of fundamental rights and freedoms, in particular the principles of necessity for interference, proportionality, and effective remedies.

28. The Venice Commission recalls that, "[w]hen a measure restricts human rights, it must be defined as precisely as possible and be necessary and proportionate to the aim pursued" (see *Guidelines of the Committee of Ministers of the Council of Europe on Human Rights and the Fight against Terrorism*, Guideline III.2). Moreover, as the Venice Commission has indicated in its *Report on counter-terrorism measures and human rights*¹⁸, "the introduction of legal provisions providing for the limitation of human rights and a fortiori for derogation from such rights, should be subjected to parliamentary approval or, in urgent cases, to posterior

¹⁵"Federal security service organs shall carry out operational/search measures for the purposes of detecting, preventing, suppressing and exposing espionage, organised crime, corruption, illegal trading of arms and drugs and smuggling presenting a threat to the security of the Russian Federation and crimes whose investigation and preliminary examination are placed within their jurisdiction by law, and also for the purposes of detecting, preventing, suppressing and exposing the activities of illegal armed formations, criminal groups, individuals and public associations aiming to forcibly change the constitutional system of the Russian Federation.

Federal security service organs may be assigned other tasks in the sphere of combating crime by federal laws and other legal and regulatory acts of federal state authorities".

¹⁶ In fields with high risks of a danger of abuse or a higher risk of violations of human rights, the ECtHR requires a higher standard of determination (see e.g. *Kruslin*, 24 April 1990, §§ 24-25; 5. 5. 2011, *Editorial Board of Pravoye Delo u. Shtekel*, 5 May 2011, §§ 63-64; see also ECtHR, *Gozelik and Others v. Poland*, No. 44158/98, 17 February 2004 and *Hasan and Chaush v. Bulgaria*, App. No. 30985/96, 26 October 2000, para 84, on the "quality of the law").

¹⁷"The State shall guarantee observance of human and civil rights and freedoms in the implementation by the Federal Security Service of its activity. The restriction of human and civil rights and freedoms shall not be permitted except in cases provided for in federal constitutional laws and federal laws".

Any person believing that their rights and freedoms have been violated by federal security service organs or their officials shall be entitled to complain of the actions of those organs and officials to a higher authority of the Federal Security Service, a prosecutor's office or a court."

¹⁸ Venice Commission, *Report on counter-terrorism measures and human rights*, CDL-AD(2010)022, 5 July 2010.

parliamentary control, while measures and action by which such limitations or derogations are applied, should be under independent review for their legality, necessity and proportionality". The general principles of legality, necessity and proportionality concern both the legislation itself and its implementation in practice. In other words, it is fundamental, in order to ensure effective protection of fundamental rights, that FSB organs and officers take adequately into account in their action - in particular when implementing legislative provisions allowing limitations to such rights - the requirements of necessity and proportionality, and that their action is subject to independent control.

B. Monitoring and supervision of the FSB activities

29. As the Commission noted in its report on Democratic Oversight of the Security Services, "Security agencies must be equipped with considerable technological tools and must enjoy exceptional powers. Governments could easily be tempted to use them to pursue illegitimate aims: for this reason, in order to prevent them from becoming an oppressive instrument for party politics, security agencies must be insulated to some degree from day-to-day political/governmental control. At the same time, this necessary insulation of security services carries with it dangers. While this should not be exaggerated, experience shows that security agencies can develop a "State within a State" mentality. A culture of regarding any non-mainstream political movement as a threat to the State can emerge. In extreme cases, an agency can manipulate the political process by infiltrating political movements, pressure groups, and trades unions, and engage in "psychological operations" and disinformation. This is a danger which is more present in some States than others. Nonetheless, a problem for the personnel of any security agency is that they can develop a "security mindset". Improved democratic scrutiny is thus not simply to protect against abuse of human rights but also to expose the intellectual assumptions and work practices of security personnel to informed criticism. Governmental control of Internal security services is therefore essential to avoid a "State within the State" mentality. It must not however be too tight – or the services may be abusively used to attain illegitimate aims" (paras 59-61)

30. The FSB exercises considerable powers, including police powers which have major implications for the human rights of citizens. The Commission noted in its Report on Democratic Oversight of the Security Services that the Parliamentary Assembly of the Council of Europe has previously expressed a clear preference for separate civilian security agencies without police powers but continued "Undoubtedly, police powers of arrest, search and seizure can, when combined in the same organization with the powers and capabilities of a security agency, create a very powerful institution. However the acceptability of such an institution from the perspective of accountability and the protection of individual rights, depends upon the adequacy of the control structure created to prevent abuse, or overuse, of power. A strong security police which is subject to tight internal controls and control by independent prosecutors, and, when authorizing special investigative measures, control by judges, cannot be said to be incompatible with Council of Europe principles in general, or the ECHR in particular" (at para. 98).

31. According to article 23 of the FSB Law, monitoring and supervision of the FSB activities is to be exercised by the President of the Russian Federation, the Federal Assembly of the Russian Federation, the Russian Federation Government and judicial bodies within the limits of their competence. In addition, individual deputies/members of the Federation Council and deputies of the State Duma of the Federal Assembly are entitled to obtain information on the FSB activity. Although under the Constitution of the Russian Federation the President is not part of the executive power (see Articles 80 and 110 of the Constitution), according to article 1 of the FSB law, "*the activity of federal security service organs shall be directed by the President of the Russian Federation*", who appoints and dismisses the head of the federal executive authority for security. While a presidential power of appointment and dismissal is acceptable, as the Commission has noted in its Report on the Democratic Oversight of the Security Services,

this is a power which can be abused and which therefore has to be subject to constraints such as confirmation or consultation procedures in the parliament (paras 135, 191). Executive directions to the agency should be in writing, so as to enable a proper "paper trail" of accountability (para. 192). It is not clear to what extent the President is involved and/or supervises operational activities of the FSB organs. It is presumably the case that the office of the Presidency has little if any time to devote to operational control over the FSB. Neither the President nor the government of the Russian Federation are, in any event, "external" controls of the FSB.¹⁹

32. A number of states provide for parliamentary oversight bodies and/or independent expert bodies for internal security agencies. The Venice Commission discussed the mandate and powers of such bodies in detail in its Report on the Democratic Oversight of Security Services (paras 149-194, 218-240).²⁰ A parliamentary or expert body serves as an important mechanism of accountability where the following criteria are satisfied; its members have developed expertise in security issues, they have access to the necessary secret information, including, where necessary, information on operations (access to classified information presupposes strict rules on due respect for secrecy on the part of the parliamentarians²¹), they attempt to hold the executive accountable for security policy and operations while at the same time not revealing information which should genuinely be kept secret, they are able to make recommendations or deliver (edited) reports proprio motu to the parliament and the public. The converse is also true: even if a parliamentary and/or expert body to oversee security exists, if it does not have the necessary powers of investigation, or if it does have such powers on paper, but it does not exercise these, or if its members have not developed sufficient expertise or if they do not act in a bipartisan manner (e.g. MPs from the party of government predominate, and regard criticism of security policy or operations as criticism of the government) then it will not be an effective oversight mechanism. Here it can be noted as regards the Russian Federation that there is a Duma committee on security and anti-corruption. However, apart from adopting the budget (or part of the budget) of the FSB, it appears to have no competence to do more than request information from the FSB. The Venice Commission has received no information that this committee exercises meaningful oversight over the FSB.²²

33. There is a "Public Council", an advisory body consisting of 15 members appointed by the Director of the FSB. According to information from the Russian representatives, this body includes members of the Public Chamber of the Russian Federation, heads of several NGOs (civil society, civil rights, charity), religious leaders, senior managers of major telecommunications, technology, transportation and banking entities. The Public Council inter alia has an advisory role in order to ensure the compliance of FSB with the constitutional rights and freedoms of the citizens of the Russian Federation and to ensure public supervision over this functioning. In the Venice Commission's opinion, such a body can be a useful channel of communication between the "closed world" of the security agency and the outside world, including civil society. However, it does not have access to confidential information, and so while it may serve several useful purposes, it cannot be described as an "oversight" body.

¹⁹ See mutatis mutandis Report on the Democratic Oversight of the Security Services, para 112: "As government departments are both "taskmasters" and "consumers" of intelligence, they cannot either be seen as an "external" control over a security agency".

²⁰ See also CDL-AD (2006)011, *Opinion on the Law on the Information and Security Service of the Republic of Moldova*, 23 March 2006 paras 149-194.

²¹ See Report on the Democratic Oversight of the Security Services, para 167.

²² The lack of effective Duma mechanisms for investigation of operations of the FSB is illustrated by the *Finogenov and Others v. Russia* case, nos. 18299/03 and 27311/03, ECtHR judgment of 20 December 2011.

34. As recognised by the Russian Federation inter alia by the establishment of the above advisory body and in the law governing the FSB (Article 6 of which, as already mentioned, requires FSB actions to comply with human rights), it is especially important that, as a rule, controls exist over the activities of security agencies when these agencies take measures, as they must do on occasion, which restrict fundamental human rights. Articles 5, 8 and Protocol 4 Article 2 of the ECHR require authority and controls over police powers such as public order powers, arrest and detention and search and seizure (including access to data held on private data banks). Moreover, as a result of ECtHR case law, there must be clear and specific legislative authority for, and satisfactory systems of control over, the following other FSB powers: the establishment and operation of the FSB's own security data banks, including access of the FSB to data from other public data banks and transfer of data from FSB security data banks to government and other authorised recipients,²³ interception of the content of communications data,²⁴ access to data specifying duration of calls, numbers calls and other identifying data concerning telecommunications, including use of the internet,²⁵ bugging, including participatory auditory surveillance,²⁶ the use of localisation devices²⁷ and the use of agents and others in infiltration.²⁸

35. The FSB use of search of citizens' homes and detention of individuals beyond 48 hours requires authorisation by a court, and the prosecutor must be informed. For the powers of interception of the content of communications and of bugging, under the Law on Operative and Search Activities, the FSB seeks court authorisation directly. Unlike in certain other states, the prosecutor does not act as a "filter" between the security agency and the courts. The need for judicial authorization for bugging and for communications interception (though not, apparently, for localization devices or to access to data specifying duration of calls, numbers calls and other identifying data) is an important safeguard for human rights.²⁹ As the Commission has noted before "The mere involvement of judges in the authorization or review process, however, is not always an effective guarantee for respect for human rights. First, the value of judicial control obviously depends upon the *independence*, in both law and fact, the judges possess from the executive in the State. This in turn depends upon the constitutional law and practices of the State in question, and its legal and political culture. Secondly, the value of judicial control depends upon the *expertise* the judges in question have in assessing risks to national security and in balancing these risks against infringements in human rights. Even for a specialised judge, the invocation of "national security" is very potent, conveying as it does

²³ Rotaru v. Romania, No. 28341/95, 4 May 2000. See also Report on the Democratic Oversight of Security Services para. 58 "The vulnerability of democratic societies combined with the diffuse nature of the threats against them means that intelligence is wanted on everything which is, or can become, a danger. Unless external limits are imposed, and continually re-imposed, then the natural tendency on all agencies is to over-collect information. Internal limits will not suffice because, while the staff of a security agency should set limits on the collection of data, it is not primarily their job to limit themselves and think about the damage which over-collection of intelligence can do to the vital values of democratic societies, in particular, the enjoyment of the rights of freedom of expression, association, privacy and to personal integrity"

²⁴ See, e.g. ECtHR, Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, No. 62540/00, 28 June 2007.

²⁵ See ECtHR, Malone v. UK, 2 August 1984, A/82, PG and JH v. UK, No. 44787/98, 25 September 2001, Copeland v. UK, No. 62617/00, 3 April 2007

²⁶ ECtHR, Heglas v. Czech Republic, No. 5935/02, 1 March 2007 (inadequacy of legal framework at the time regulating body-mounted listening devices and metering data), Bykov v. Russia, No. 4378/02, 21 January 2009.

²⁷ ECtHR, Uzun v. Germany, No. 35623/05, 2 September 2010

²⁸ ECtHR, Sequeira v. Portugal No. 73557/01, ECHR 2003-VI, Taal v. Estonia, No. 13249/02, 22 November 2005, Vanyan v. Russia, No. 53203/99, 15 December 2005, Eurofinacom v. France (dec.), No. 58753/00, ECHR 2004-VII, Khudobin v. Russia, No. 59696/00, 26 October 2006.

²⁹ Report on the Democratic Oversight of Security Services para. 204: "there is an obvious advantage of requiring prior judicial authorization for special investigative techniques, namely that the security agency has to go "outside of itself" and convince an independent person of the need for a particular measure".

a need for urgent and decisive action...It is likely to be a strong-minded judge with considerable prior experience of dealing with previous applications who is able to question the proportionality of the experts' assessments and stand firm against the temptation to balance away integrity almost every time. Psychologically speaking, a tendency to grant authorizations is likely to be strengthened where the State, for example for reasons of separation of powers, has no procedure for checking up on, let alone criticizing, the number and duration of judicial authorizations granted"³⁰.

36. The Venice Commission will content itself with noting that the judges are obliged under the ECHR to scrutinize, critically, applications for the use of special investigative measures from the FSB. This should mean, even allowing for a high degree of professionalism from the FSB in preparing applications, that at least some applications are denied. The ECtHR has set high standards in this respect.³¹ The same point can be made as regards the more general power which individuals have to complain to the courts of unlawful activities by the FSB under Article 6 of the FSB law: the relevant ECtHR case-law requires that remedies not only exist on paper but function in practice.³²

37. In the Russian Federation, as in many other states, a number of important security powers, above all, that of gathering intelligence on individuals is not directly supervised by the courts. The main system of control over the FSB is provided by the prosecutor's general power of supervision under Article 1 of the Federal Law on the Prosecution Service³³ and Article 24 of the FSB law,³⁴ as well as a specific power of supervision over the FSB's use of "operative and search" activities.³⁵ There is a group of security-screened prosecutors who exercise these powers in practice.

38. Prosecutors must obviously have sufficient expertise in security matters, and sufficient authority, to be able to act as a real control over the – of necessity - closed world of the internal security agency. This means inter alia a degree of specialisation. However, there are dangers in this too. As the Commission noted, referring in particular to specialist security judges, but also to prosecutors, there is a risk of "case hardening". "The group of security cleared judges and prosecutors can be so small that it is almost "incestuous", and they may

³⁰ Report on Democratic Oversight over Security Services, paras 205-206, 208. See also para. 213, where the Commission, recommended for states which have judicial authorization "that some form of appeal or follow-up mechanism should exist for even judicial authorization of special investigation techniques. It also suggests that, unless special reasons exist, the number of years spent as a judge authorising or reviewing security surveillance should not be too long."

³¹ See the criticism of the ECtHR in *Association for European Integration and Human Rights and Ekimdzhiiev v. Bulgaria*, op. cit and in *Lordachi and others v. Moldova*, No. 25198/02, 10 February 2009, at para. 51 where the ECtHR noted that there was a lack of safeguards in the law combined with a very high percentage of authorisations issued by the investigating judges combined ("For the Court, this could reasonably be taken to indicate that the investigating judges do not address themselves to the existence of compelling justification for authorising measures of secret surveillance").

³² See in particular ECtHR, *Segerstedt-Wiberg v. Sweden*, No. 62332/00, 6 June 2006,.

³³ Federal law on the prosecutor's office of the Russian Federation of 17 January 1992, as amended; http://eng.genproc.gov.ru/legal_basis_of_the_activities/document-13082/

³⁴ According to information received from the Russian Federation, the new investigative committees do not exercise standing supervision over the FSB. They would, however, investigate allegations that a crime had been committed by FSB personnel.

³⁵ Federal law on the prosecutor's office of the Russian Federation of 17 January 1992, as amended, Article 29 provides "Supervision shall be exercised to ensure the observance of human and civil rights and freedoms, compliance with the prescribed procedure for dealing with statements and reports concerning planned or committed crimes, for carrying out operative-and-search measures and conducting investigations, and also to ensure the legality of any decisions taken by bodies carrying out operative-and-search activities, inquiries and preliminary investigations"; http://eng.genproc.gov.ru/legal_basis_of_the_activities/document-13082/.

come to identify more with the people with whom they are in daily contact – the security officials – rather than their judicial colleagues. There is a danger that these judges become so used to the types of techniques, information and assessments they see every day that they lose their qualities of independence and external insight through a process of acclimatisation. The necessary awareness of the suspect's rights may gradually be lost over the years spent in the isolated world of security intelligence.³⁶

39. The prosecutor may either act proactively, first finding out whether a special investigative power has been used, then demanding to see the file in question, or the prosecutor may demand the file in response to a complaint. As Article 7 of the Law on Operative and Search Activities (and the FSB Law) also provides authority for the FSB to gather and process intelligence on individuals, the prosecutor also has a supervisory role over the FSB's security files. If a citizen complains that intelligence is being unlawfully gathered about him or her, the prosecutor may demand the production of the file (if there is one) and determine if the law is being complied with, including whether the individual's rights are being respected (which should also involve a proportionality control). The prosecutor's right to demand the production of the information they request from the FSB is subject to an exception, under Article 24 of the FSB Law, namely "information on persons having provided or providing assistance to federal security service organs on a confidential basis" (i.e. informers). This exception is not unusual in security contexts, even if situations can presumably arise where, to determine the reliability of the information on which the FSB has acted, it may be necessary to give access to data confirming the reliability of the source. Article 24 also provides a more general exception namely information "on the organization, tactics, methods and means used by federal security service organs to carry out their activity".

40. However, the main question-mark regarding the prosecutor as the primary means of supervision of the FSB does not concern the above exceptions, nor the authority and powers of the prosecutor but rather the independence of the prosecutor. While accepting, in principle, that a security agency with police powers can be controlled by prosecutors, the Commission in its Report on the Democratic Oversight of Security Services stressed that prosecutorial independence must exist both in law and in fact. The Commission stated that "Depending upon the constitutional structure and legal culture of the State, prosecutors possess varying degrees of independence from both the agency and government direction and can be a useful control over the security agency, to the extent that its work involves gathering evidence for prosecution. However, prosecutors in a State which are not, formally and in practice, a part of the independent judicial branch are nonetheless a part of the executive and as such can only be seen as an "internal" control" (para. 110).

41. The Commission has previously scrutinized the Federal Law on The Prokuratura (Prosecutor's Office) of the Russian Federation of 17th January 1992 (as amended).³⁷ The Commission noted that the "position of individual prosecutors with respect to their superiors seems weak and not in compliance with [Committee of Ministers] Recommendation (2000) 19 ... it seems that dismissal is by decision of the head – there is no provision for appeal at least in this Law" (at para. 70). It noted the Prosecutor General "has complete power to issue binding orders to the entire Procuracy, that he appoints and dismisses the key figures ... that the Prosecutor General cannot be removed unless the President seeks his removal and that the criteria for removal are not specified" (para. 60). It considered that the extent of the Prosecutor General's power is very great indeed. Furthermore, the Commission pointed to the relationship between the Procuracy and the Presidency.

³⁶ Report on Democratic Oversight over Security Services, para 213.

³⁷ CDL-AD(2005)014 Opinion on the Federal Law on The Prokuratura (Prosecutor's Office) of the Russian Federation.

42. In the light of the above, the Venice Commission has serious doubts that the supervision of the FSB by the prosecutors should qualify as an "external" mechanism of control.

C. FSB powers under the 2010 amendments - The preventive measures

a) Generally

43. As previously indicated, Article 13.1 of the Law on the FSB as amended provides the following:

"Preventive measures used by the federal security service authorities shall include the lodging of a request to eliminate causes and conditions facilitating the carrying out of threats to the security of the Russian Federation and the issuing of an official warning, with which compliance is mandatory, of the inadmissibility of actions creating conditions for the committing of crimes for which detection and preliminary investigation is placed by Russian Federation legislation within the jurisdiction of the federal security service authorities.

In the presence of sufficient elements uncovered in the operational activities of the federal security service authorities which point to causes and conditions facilitating the carrying out of threats to the security of the Russian Federation, the federal security service authorities shall lodge with the corresponding state authorities or administrations of enterprises, institutions and organisations, regardless of their form of ownership, and also with public organisations, a request, with which those bodies are bound to comply, to eliminate said causes and conditions facilitating the carrying out of threats to the security of the Russian Federation.

[...]

A request to eliminate causes and conditions facilitating the carrying out of threats to the security of the Russian Federation or an official warning of the inadmissibility of actions creating conditions for the committing of crimes for which detection and preliminary investigation is placed by Russian Federation legislation within the jurisdiction of the federal security service authorities may be appealed against before a court and the authorities indicated in Article 6 of the present Federal Law".

44. At the same time, through the Federal Law No. 238-FZ, an amendment was also made to the Code of Administrative Offences of the Russian Federation, which Article 19.4 now contains the following provision:

*"4. Failure to obey a lawful order or request given or made by an officer of the federal security service authorities in the performance of their duties and also hindering an officer in the performance of their duties
- shall be punishable by an administrative fine in the case of a citizen of between five hundred and one thousand roubles or administrative arrest for a period of up to fifteen days; or a fine of between one thousand and three thousand roubles in the case of an official; or a fine of between ten thousand and fifty thousand roubles in the case of a legal person."*

45. The Venice Commission will begin by noting that the Russian Federation is the object of extremely serious threats in relation to internal and external terrorism, organized crime and/or manifestations of extremism. The Venice Commission has already stated in the past that the security of the State and its democratic institutions, as well as the safety of its population, are a legitimate aim and represent vital public and private interests that deserve protection, if necessary at high costs³⁸. As the ECtHR has held, the protection of the right to life "may also

³⁸ Cf. CDL-AD(2006)015, Opinion on the Protection of Human Rights in Emergency Situations, § 5.

*imply in certain well-defined circumstances a positive obligation on the part of the authorities to take preventive operational measures to protect an individual whose life is at risk from the criminal acts of another individual*³⁹.

46. However, States not only have the duty to protect state security, and the individual and collective safety of their inhabitants; they also have the duty to protect the (other) rights and freedoms of those inhabitants.⁴⁰ The Venice Commission recalls that, according to article 2 of the Constitution of the Russian Federation “[m]an, his rights and freedoms are the supreme value”.

47. Article 13.1 thus provides FSB with competences and powers in relation to the use of two instruments as specific forms of preventive measures: issuing official warnings to individuals and formal requests to organisations, including non-governmental organisations whose actions are deemed to be creating the conditions for crime. The Venice Commission will deal first with warnings.

b) Official warnings to physical persons

48. The instrument may be used for the purpose of preventing the committing of crimes for which detection and preliminary investigation is placed with the FSB (above, para. 25). Warnings are meant to be used in cases of conduct which is preparatory to crime, but not sufficient to be criminalized under Article 30 of the Criminal Code. The warning serves the purpose of putting the subject on notice that s/he is “approaching the criminalized area”. One situation in which a warning might be issued is where the FSB discovers that an individual has announced on the internet his intention to commit a terrorist act. The Law does not specify exactly what information is required before a warning can be issued, referring only to “objectively and materially ascertainable facts”. However, Federal Security Service Order no. 544 of 2 November 2010 (CDL-REF(2012)022) provides some more detail in this respect. Para. 3 of Annex I of the order provides that “The presence of sufficient and duly and previously confirmed information on specific acts of physical individuals creating conditions for the committing of crimes shall provide grounds for issuing an official warning: outwardly showing (verbally, in writing or in some other manner) the intention to commit a distinct crime in the absence of any indication of the preparation of the crime or an attempt to commit the crime; establishing preparations for a crime of minor or medium gravity or directly aimed at the committing of such crimes in the absence of any indication of an attempt to commit the crime”. The order also specifies (in appendix 2) which officials in the FSB may issue a warning. This consists of senior officials.⁴¹

³⁹ ECtHR, *Osman v. United Kingdom*, Judgment of 28 October 1998, § 115 and ECtHR, *LCB v. UK*, Judgment of 9 June 1998, §36.

⁴⁰ See Preamble of the Council of Europe Convention on the Prevention of Terrorism, CETS No. 196: See also CDL-AD(2007)016, Report on the Democratic Oversight of the Security Services: “The protection of internal security must include the protection of the fundamental values of the State which, for a liberal democratic State, means inter alia democracy and human rights: However, in practice, the values of freedom and security can easily be perceived as opposing values” §58.

⁴¹ “Director of the FSB of Russia; deputies of the Director of the FSB of Russia, heads of services of the FSB of Russia and their deputies, heading/supervising sub-divisions of the FSB of Russia, authorised to carry out operational/search activities; heads and chief administrators of departments, centres and directorates of the FSB of Russia, and of directorates of services and centres of the FSB of Russia, authorised to carry out operational/search activities; chief administrators of directorates of the FSB of Russia covering individual regions and constituent entities of the Russian Federation; chief administrators of directorates and heads of department holding equivalent powers of the FSB of Russia within the Armed Forces of the Russian Federation, other forces and military units and their administrative bodies; heads of the border service directorates of the FSB of Russia”.

49. The responsible officials are to take a decision as to whether to issue an official warning within ten days after they have been informed about the possible threat from a person or group of persons, and issue the warning to the individual concerned no later than 5 days from the date of the decision. Federal Security Service Order no. 544 provides for clear routines for ensuring that physical persons are notified of warnings and for registering warnings.

50. Under the final paragraph of article 13.1, the requests and warnings in question "may be appealed against before a court and the authorities indicated in article 6 of the present Federal Law" (i.e. a more senior level of the FSB and a prosecutor's office)⁴².

51. The Law specifies that the prosecutor must be informed first. Only after that step an "official warning" may be issued. One of the purposes of this is to give the prosecutor the opportunity to determine whether the act has, in fact, already crossed the threshold into the criminalized area. The use of a warning is thus subsidiary to the criminal law.

52. The Venice Commission has been informed, that, since 2010, only 26 warnings have been issued. No appeals against these have been made to the courts, the ombudsman or the prosecutors.

53. A number of issues arise in connection with warnings. The wording of the English translation of the provision – "compliance is mandatory" – together with the change which was made to Article 19.4 of the Code of Administrative Offences can give the impression that an administrative penalty is applicable in the event that the FSB consider that the warning has not been complied with. However, a warning does not fall within the definition of "official order or request" under Article 19.4 (see further below, para 62). Thus, there is no administrative penalty for non-compliance with a warning. However, according to information received by the representatives of the Russian Federation, if there is a later criminal prosecution, and the court considers that a crime has been committed, in sentencing, the court will take into account all the circumstances of the case. Thus, the fact that a warning has been issued and not complied with can be taken into account in sentencing (though it does not serve to convert an offence into an aggravated offence).

54. The "Explanatory note" to this amendment, which is an integral part of the law and which thus is binding, can also, in its English translation, cause some confusion. It provides that "[t]he provisions of paragraph 4 of the present article shall not apply to citizens in the event of preventive measures being taken against them in accordance with the Federal Law "On the Federal Security Service". This provision, introduced in the final text of the amendment adopted in 2010, appears to deal only with the *imposition* of the penalty, not its *applicability*, and, moreover, only as regards citizens. However, the purpose of this provision is only to make it doubly clear that non-compliance with a warning is not backed by a penalty, and the Russian Federation government assures the Venice Commission that the use of the word "citizen" does not mean *e contrario* that penalties *are* applicable to non-citizens.

⁴² According to Article 6 of the FSB law: « [...]Any person believing that their rights and freedoms have been violated by federal security service organs or their officials shall be entitled to complain of the actions of those organs and officials to a higher authority of the Federal Security Service, a prosecutor's office or a court. (as per Federal Law No. 15-FZ of 07.03.2005)

[...]In the event of a violation of human and civil rights and freedoms by federal security service organ staff, the head of the respective federal security service organ, a prosecutor or a judge shall be bound to take measures to restore those rights and freedoms, grant compensation for the damage caused and prosecute the perpetrators as provided for in Russian Federation legislation.

Federal security service organ officials misusing their authority or exceeding their official powers shall incur liability as provided for in Russian Federation legislation.

(as per Federal Law No. 15-FZ of 07.03.2005)"

55. The question arises, despite the absence of a penalty, whether warnings can be criticized on other grounds. Here it should be noted that other states might also permit their security bodies to contact people who are believed to be involved in, or planning, security crime, and to warn them informally. By formalizing the use of warnings, the Russian Federation allows a degree of transparency in the use of the device. Moreover, the fact that only certain officials in the FSB may issue warnings means that there is a proper "paper trail" – assuming the clear routines of registration etc. set out in Federal Security Service Decree no. 544 are properly followed by all this group of officials in practice.

56. On the other hand, a warning means that a certain "grey zone" between what is legal and not legal has been created. Warnings have to be seen together with legislation dealing with "speech crimes", especially offences criminalizing extremist speech. The Venice Commission considers that in a democratic society it is crucially important to try to maintain a relatively clear dividing line between activities which are not simply desirable, but vitally necessary for the maintenance of this society (such as freedom of speech) and dangerous behaviour which, for one or other reason, society has found necessary to criminalize. In general it can be noted that if a state has already enacted legislation which places strong limits on the rights of freedom of expression and association, then a warning, being a preventive measure, and so dealing with "pre-crime", risks going beyond the restrictions permissible under the ECHR. It is inevitable that a security agency, even if it acts with professionalism, will not always be correct in its risk assessment that person X, or phenomenon Y in concrete circumstances Z constitutes a threat to the state. On the contrary, it should be recollected that security agencies have a natural tendency to "err on the side of caution" and over-assess threats.⁴³ Thus, if mistakes are made, or overuse occurs, then this can and will "chill" legitimate exercises of the rights of freedom of expression and association.

57. Seen in this perspective, the concept of the criminal law is itself a safeguard for human freedom. If, and only if, something is sufficiently dangerous to society, can the legislature choose to criminalize it. Moreover, certain material and procedural conditions must be fulfilled in the criminal law in a society governed by the rule of law. The dangers posed by terrorism are real; however, the risk of mistaken application of terrorist offences against innocent people who for one reason or another are suspected of having "evil intentions" is also real.

58. In general, security offences have a tendency to "begin" early. When combined with the general part of the criminal law (attempt, conspiracy, aiding and abetting), relatively little may be required in the way of concrete suspicion that a specific security offence is ongoing. As a general issue of criminal policy, any offence introduced to deal with terrorism (and, *mutatis mutandis*, any other security offence) may not simply criminalize subjective intent, but must also address "actual facts which it must be possible to ascertain materially and objectively".⁴⁴ The Russian Federation is a party to the Council of Europe Convention on the Prevention of Terrorism and also has a battery of legislation criminalizing preparation etc. of terrorism and other security offences. Thus, any overt act in furtherance of a security or terrorist offence is, together with the necessary criminal intent, likely already to be a criminal offence. The Russian warning system differs from, e.g. the UK system of "official notices" issued under section 2 of the Prevention of Terrorism Act 2006, in relation to internet material considered to be inciting or glorifying terrorism. The publication of this material is already a criminal offence, but the person who is formally in charge of an internet site may not in fact have posted the material in question, and may not agree with the views expressed in it. Here the object of the notice is to inform the

⁴³ CDL-AD(2007)016, para. 58 "Unless external limits are imposed, and continually re-imposed, then the natural tendency on all agencies is to over-collect information. Internal limits will not suffice because, while the staff of a security agency should set limits on the collection of data, it is not primarily their job to limit themselves and think about the damage which over-collection of intelligence can do to the vital values of democratic societies". See also §§ 86 and 208.

⁴⁴ Venice Commission, *Report on counter-terrorism measures and human rights*, CDL-AD(2007) para. 32.

person of the criminal nature of the material and to inform him/her that failure to remove it speedily will mean that s/he will be regarded as endorsing the material, and so be liable to prosecution.

59. While a state party to the ECHR has a broad discretion as to what to criminalize, and how to go about doing so, when criminalization encroaches upon the protected area of rights, this discretion is not unlimited. The ECtHR in a large number of cases has discussed the standards necessary to satisfy the "accordance with the law" requirement in the Convention. As the Court stated, "[t]he level of precision required of domestic legislation - which cannot in any case provide for every eventuality - depends to a considerable degree on the content of the instrument in question, the field it is designed to cover and the number and status of those to whom it is addressed"⁴⁵. The area of criminal law, or in this case, quasi-criminal law, requires a high degree of precision. The *Gillan and Quinton* case concerned a power to stop and search a pedestrian, without reasonable suspicion, if a police officer considered it "expedient for the prevention of acts of terrorism". There are thus some parallels with Article 13.1. The Court found "a clear risk of arbitrariness in the grant of such a broad discretion to the police officer ... There is, furthermore, a risk that such a widely framed power could be misused against demonstrators and protestors in breach of Article 10 and/or 11 of the Convention" (§ 85).

60. Although a warning may be appealed to a higher level of the FSB, a prosecutor's office, or the courts as indicated above (para 49) only the courts fulfil the requirements of Article 6 ECHR. Unlike the situation in relation to an official request (below para 68) it is not clear what an appeal can accomplish in practice in relation to a warning. As already noted, even when a formal possibility of appeal exists, courts, in Russia like elsewhere, tend to experience difficulties in practice in questioning the experts' determinations that a given conduct is a security threat.

61. Warnings in any event appear to have been used sparingly (above para. 52). As explained above, the acceptability of warnings depends upon whether they are "chilling", or potentially can "chill", the exercise of rights protected under the Russian constitution and the ECHR, in particular under Articles 9 to 11 ECHR. The Venice Commission will thus content itself with noting that whether or not warnings are in compliance with the ECHR will depend in how they are, now and in the future, used in practice.

c) Requests to legal persons

62. An official request can be issued "to eliminate causes and conditions facilitating the carrying out of threats to the security of the Russian Federation". The concerned organisations are "bound to comply" with the request which is thus an order. Unlike a warning, a request is backed by an administrative penalty under Article 19.4 of the Code of Administrative Offences which is applicable if the request is not complied with.

63. The request can be directed against "establishments, organisations, regardless of their ownership", i.e. both public and private bodies.

64. It is not difficult to understand how the English translation of the basis for issuing a request can give rise to disquiet. Moreover, the fact that private companies, and NGOs, may be the subject of official requests can also raise questions. In its English translation, the basis for the request can be read as permitting the FSB to prescribe conduct in the future, perhaps even in an area protected by a fundamental right, such as freedom of expression. Here reference can usefully be made to the Court's judgment in *Hashman and Harrup v. UK*,⁴⁶ concerning the

⁴⁵ *Gillan and Quinton v. UK*, Application No. 4158/05, 12 January 2010, para 77.

⁴⁶ No. 25594/94 25 November 1999.

power of a magistrate to “bind over” a person “to be of good behaviour”, in which the Court noted that “It is a feature of the present case that it concerns an interference with freedom of expression which was not expressed to be a “sanction”, or punishment, for behaviour of a certain type, but rather an order, imposed on the applicants, not to breach the peace or behave *contra bonos mores* in the future. The binding-over order in the present case thus had purely prospective effect” (§ 35). The ECtHR went on to find a violation of the Convention, notwithstanding the fact that the order was made by a judicial officer (a magistrate).

65. However, if one instead reads the competence to issue an official request as closely linked to, and limited by, the FSB competence to investigate serious security crimes, it is clear that official requests, even when backed by a penalty, have a legitimate area of application.

66. Moreover, even outside of the area of investigation into specific security crimes, in dealing with the more general of responsibility of the FSB to prevent security crime, there can be a legitimate area of application of the provision *as regards government departments and administrative agencies*. Combating corruption is within the competence of the FSB. It is well-known that, both in states where there is a civil security agency and in states with a security police, a part of their work is identifying structural security vulnerabilities in government agencies. These vulnerabilities can also have to do with staff organisation and training in various ways (openness to bribery by organised crime, agents of foreign powers etc.), in particular as regards procurement, but also physical security against, e.g., terrorism and infrastructure security, in particular vulnerability to cyber attacks. Where there is a pre-existing legal obligation for government departments or administrative agencies to maintain a high degree of physical and cyber-security, reduce vulnerabilities to corruption etc. then it is obviously legitimate for the FSB to point out vulnerabilities in structures and routines etc. and to require corrective measures to be taken, backed by an administrative penalty. In some European states, offences constructed in a similar way can be found in certain regulatory areas of law, such as environmental law: where an inspector considers that regulations on, e.g. emission of harmful chemicals, are not being followed, s/he can specify corrective measures to be taken within a period of time. Failure to comply with this order may be punishable by a fine (appealable, or reviewable, by a court). However, it should be stressed that this is to ensure compliance with an *existing* and *objectively verifiable* legal duty (not to pollute the environment, to provide a safe working place etc.).

67. The problem with official requests is the same as with warnings, namely the wide basis for issuing official requests which, actually or potentially, can include official requests concerning activity protected by fundamental rights, in particular the freedoms of association and expression. Companies and associations are entitled to these (and certain other) rights under the ECHR.⁴⁷ An administrative fine applies for non-compliance, which makes the potentially chilling effect even more apparent (even if, as follows from the wording of Article 19.4 of the Code of Administrative Offences, the penalty of imprisonment may not be imposed upon an officer of a corporation, association or other legal person).

68. The safeguard against this is the possibility of appeal, under article 6 of the FSB Law, to a higher level of the FSB, the prosecutor and the courts. As already noted, only the courts fulfil the requirements of Article 6 ECHR. As already noted in connection with warnings (above para 60) courts experience difficulties in practice in reviewing security decisions. With official requests, however, the right of appeal serves a more obvious purpose, as the courts, applying the principles of legality and proportionality formally speaking have the competence to annul the request and/or vary or annul the penalty. The Venice Commission will, again, content itself with noting that the wide formulations used in the law (“to eliminate causes and conditions facilitating the carrying out of threats to the security of the Russian Federation”) means that there is a

⁴⁷ See e.g. *Comingersoll S.A. v. Portugal*, No. 35382/97, 6 April 2000.

potential for official requests backed by penalties to be used outside of their legitimate spheres of application. If, now or in the future, official requests are used to prescribe conduct for associations or corporations which would interfere with their fundamental rights of freedom of association or expression, then this would not be in accordance with the ECHR.

IV. Conclusions

69. The Venice Commission stresses at the outset that it is commonly accepted that the development of more efficient means and measures to safeguard the state's security and ensure its citizens' protection against the dangers of extremism, terrorism or organised crime represents in itself a legitimate aim. However, the protection and respect of fundamental rights represents an essential condition for the operation of security services as part of a democratic society and requires solid and specific guarantees.

70. The Venice Commission has examined the text of the Law on the Federal Security Service (FSB). It finds that it calls for the following remarks:

- a) As regards the legal basis governing the activities of FSB organs, it is defined in the Law with reference to the Constitution and several other legal texts, including the code of criminal procedure. It would be useful if the Law contained an explicit requirement to duly respect the principles of necessity and proportionality and to provide for effective remedies.
- b) As regards the monitoring and supervision of the FSB activities, the Venice Commission has previously indicated as a general rule that firstly it is necessary to establish mechanisms to prevent political abuse while providing for effective governance of the agencies. Overall, the objective is that security and intelligence agencies should be insulated from political abuse without being isolated from executive governance. Secondly the rule of law must be respected. Agencies must be subject to legal control. As in other areas of public administration, one key task of the parliament is, by means of statute, to delegate authority to the executive but also to structure and confine discretionary powers in law. The challenge for oversight and accountability is to adapt or devise processes that command democratic respect at the same time as protecting national security. At the level of review, it is absolutely necessary to have external mechanisms to bridge the barrier of secrecy and provide assurance for the executive, legislators and the public that operations are being carried out effectively, lawfully and in accordance with policy.

In Russia, oversight of the FSB is exercised by the President of the Russian Federation, the Federal Assembly, the government and the judicial bodies. The President and the government are not "external" controls. The Duma Committee on security and anti-corruption, besides adopting the budget or part of the budget of the FSB, seems to be empowered merely to request information. A "Public Council" with an advisory role in order to ensure the compliance of FSB with the constitutional rights and freedoms of the citizens, may be a useful channel of communication but, in the Venice Commission's view, it cannot be described as an oversight body, notably because it does not have access to confidential information. Judicial control, both preventive and subsequent, of individual measures may instead represent a safeguard for human rights, provided that the judges possess an appropriate level of expertise and experience. As concerns the control of the gathering of intelligence and the use of operative and search activities, it is carried out by specialised, security-screened prosecutors. While prosecutors may indeed represent a useful control over the security agency to the extent that its work involves gathering evidence for the prosecution, the Venice Commission has previously stated that prosecutors may only be seen as an "external" control if they are formally and in practice a part of the independent judicial branch. The Venice Commission has

previously found that the Russian prosecutors are strongly subjected to the hierarchical control of their superiors and of the Prosecutor-General. Against this background, the Venice Commission has serious doubts that they represent a mechanism of "external" control.

- c) As regards the prevention measures, official warnings addressed to individuals do not carry sanctions and may be appealed also in court. Nevertheless, they intervene in a "grey zone" situated between what is legal and what is illegal, and may be used in an arbitrary manner, thus risking having an undue chilling effect on the exercise of fundamental rights and freedoms. Requests addressed to organisations instead do carry sanctions and, although they may be appealed, their potential chilling effect is even greater. In the Venice Commission's view, therefore, the preventive measures set out in the Law have the potential to impinge on fundamental rights, depending on how they are applied in practice.

Exhibit O

- (d) in section 78(3), for paragraph (b) there were substituted –
 - “(b) in the case of communications data which does not fall within paragraph (a) above but does fall within paragraph (c) of the definition of “communications data” in section 224(3), the day on which the person concerned leaves the postal service concerned or (if earlier) the day on which the data is changed,” and
 - (e) in section 78(9), the words from “and this expression” to the end were omitted.
- 5
- 86 **Extra-territorial application of Part 4** 10
- (1) A retention notice, and any requirement or restriction imposed by virtue of a retention notice or by section 81, 82 or 84(1) to (3), may relate to conduct outside the United Kingdom and persons outside the United Kingdom.
 - (2) But section 84(5), so far as relating to those requirements or restrictions, does not apply to a person outside the United Kingdom. 15
- 87 **Part 4: interpretation**
- (1) In this Part –
 - “notice” means notice in writing,
 - “relevant communications data” has the meaning given by section 78(9),
 - “retention notice” has the meaning given by section 78(1). 20
 - (2) See also –
 - section 223 (telecommunications definitions),
 - section 224 (postal definitions),
 - section 225 (general definitions),
 - section 226 (index of defined expressions). 25

PART 5

EQUIPMENT INTERFERENCE

Warrants under this Part

- 88 **Warrants under this Part: general**
- (1) There are two kinds of warrants which may be issued under this Part – 30
 - (a) targeted equipment interference warrants (see subsection (2));
 - (b) targeted examination warrants (see subsection (9)).
 - (2) A targeted equipment interference warrant is a warrant which authorises or requires the person to whom it is addressed to secure interference with any equipment for the purpose of obtaining – 35
 - (a) communications (see section 118);
 - (b) equipment data (see section 89);
 - (c) any other information.
 - (3) A targeted equipment interference warrant –

- (a) must also authorise or require the person to whom it is addressed to secure the obtaining of the communications, equipment data or other information to which the warrant relates;
 - (b) may also authorise that person to secure the disclosure, in any manner described in the warrant, of anything obtained under the warrant by virtue of paragraph (a). 5
- (4) The reference in subsections (2) and (3) to the obtaining of communications or other information includes doing so by—
- (a) monitoring, observing or listening to a person’s communications or other activities; 10
 - (b) recording anything which is monitored, observed or listened to.
- (5) A targeted equipment interference warrant also authorises the following conduct (in addition to the conduct described in the warrant)—
- (a) any conduct which it is necessary to undertake in order to do what is expressly authorised or required by the warrant, including conduct for securing the obtaining of communications, equipment data or other information; 15
 - (b) any conduct by any person which is conduct in pursuance of a requirement imposed by or on behalf of the person to whom the warrant is addressed to be provided with assistance in giving effect to the warrant. 20
- (6) A targeted equipment interference warrant may not, by virtue of subsection (3), authorise or require a person to engage in conduct, in relation to a communication other than a stored communication, which would (unless done with lawful authority) constitute an offence under section 2(1) (unlawful interception). 25
- (7) Subsection (5)(a) does not authorise a person to engage in conduct which could not be expressly authorised under the warrant because of the restriction imposed by subsection (6).
- (8) In subsection (6), “stored communication” means a communication stored in or by a telecommunication system (whether before or after its transmission). 30
- (9) A targeted examination warrant is a warrant which authorises the person to whom it is addressed to carry out the selection of protected material obtained under a bulk equipment interference warrant for examination, in breach of the prohibition in section 170(4) (prohibition on seeking to identify communications of, or private information relating to, individuals in the British Islands). 35
- In this Part, “protected material”, in relation to a targeted examination warrant, means any material obtained under a bulk equipment interference warrant under Chapter 3 of Part 6, other than material which is— 40
- (a) equipment data;
 - (b) information (other than a communication or equipment data) which is not private information.
- (10) For provision enabling the combination of targeted equipment interference warrants with certain other warrants or authorisations (including targeted examination warrants), see Schedule 8. 45
- (11) Any conduct which is carried out in accordance with a warrant under this Part is lawful for all purposes.

89 Meaning of “equipment data”

- (1) In this Part, “equipment data” means –
 - (a) systems data;
 - (b) data which falls within subsection (2).
- (2) The data falling within this subsection is identifying data which – 5
 - (a) is, for the purposes of a relevant system, comprised in, included as part of, attached to or logically associated with a communication (whether by the sender or otherwise) or any other item of information,
 - (b) is capable of being logically separated from the remainder of the communication or the item of information, and 10
 - (c) if it were so separated, would not reveal anything of what might reasonably be considered to be the meaning (if any) of the communication or the item of information, disregarding any meaning arising from the fact of the communication or the existence of the item of information or from any data relating to that fact. 15
- (3) In subsection (2), “relevant system” means any system on or by means of which the data is held.
- (4) For the meaning of “systems data” and “identifying data”, see section 225.

90 Subject-matter of warrants

- (1) A targeted equipment interference warrant may relate to any one or more of the following matters – 20
 - (a) equipment belonging to, used by or in the possession of a particular person or organisation;
 - (b) equipment belonging to, used by or in the possession of a group of persons who share a common purpose or who carry on, or may carry on, a particular activity; 25
 - (c) equipment belonging to, used by or in the possession of more than one person or organisation, where the interference is for the purpose of a single investigation or operation;
 - (d) equipment in a particular location; 30
 - (e) equipment in more than one location, where the interference is for the purpose of the same investigation or operation;
 - (f) equipment which is being, or may be used, for the purposes of a particular activity or activities of a particular description;
 - (g) equipment which is being, or may be used, to test, maintain or develop capabilities relating to interference with equipment for the purpose of obtaining communications, equipment data or other information; 35
 - (h) equipment which is being, or may be used, for the training of persons who carry out, or are likely to carry out, such interference with equipment. 40
- (2) A targeted examination warrant may relate to any one or more of the following matters –
 - (a) a particular person or organisation;
 - (b) a group of persons who share a common purpose or who carry on, or may carry on, a particular activity; 45
 - (c) more than one person or organisation, where the conduct authorised by the warrant is for the purpose of a single investigation or operation;

- (d) the testing, maintenance or development of capabilities relating to the selection of protected material for examination;
- (e) the training of persons who carry out, or are likely to carry out, the selection of such material for examination.

Power to issue warrants

5

91 Power to issue warrants to intelligence services: the Secretary of State

- (1) The Secretary of State may, on an application made by or on behalf of the head of an intelligence service, issue a targeted equipment interference warrant if—
 - (a) the Secretary of State considers that the warrant is necessary on grounds falling within subsection (5), 10
 - (b) the Secretary of State considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by which conduct,
 - (c) the Secretary of State considers that satisfactory arrangements made for the purposes of sections 112 and 113 (safeguards relating to disclosure etc.) are in force in relation to the warrant, and 15
 - (d) except where the Secretary of State considers that there is an urgent need to issue the warrant, the decision to issue the warrant has been approved by a Judicial Commissioner.

- (2) But the Secretary of State may not issue a targeted equipment interference warrant under subsection (1) if—
 - (a) the Secretary of State considers that the only ground for considering the warrant to be necessary is for the purpose of preventing or detecting serious crime, and
 - (b) the warrant, if issued, would authorise interference only with equipment which would be in Scotland at the time of the issue of the warrant or which the Secretary of State believes would be in Scotland at that time. 25

For the power of the Scottish Ministers to issue a targeted equipment interference warrant, see section 92. 30

- (3) The Secretary of State may, on an application made by or on behalf of the head of an intelligence service, issue a targeted examination warrant if—
 - (a) the Secretary of State considers that the warrant is necessary on grounds falling within subsection (5),
 - (b) the Secretary of State considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct, 35
 - (c) the Secretary of State considers that the warrant is or may be necessary to authorise the selection of protected material for examination in breach of the prohibition in section 170(4) (prohibition on seeking to identify communications of, or private information relating to, individuals in the British Islands), and 40
 - (d) except where the Secretary of State considers that there is an urgent need to issue the warrant, the decision to issue the warrant has been approved by a Judicial Commissioner. 45

- (4) But the Secretary of State may not issue a targeted examination warrant under subsection (3) if the warrant, if issued, would relate only to a person who

would be in Scotland at the time of the issue of the warrant or whom the Secretary of State believes would be in Scotland at that time.

For the power of the Scottish Ministers to issue a targeted examination warrant, see section 92.

- (5) A warrant is necessary on grounds falling within this subsection if it is necessary— 5
- (a) in the interests of national security,
 - (b) for the purpose of preventing or detecting serious crime, or
 - (c) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security. 10
- (6) A warrant may be considered necessary on the ground falling within subsection (5)(c) only if the interference with equipment which would be authorised by the warrant is considered necessary for the purpose of obtaining information relating to the acts or intentions of persons outside the British Islands. 15
- (7) The matters to be taken into account in considering whether the conditions in paragraphs (a) and (b) of subsection (1) are met include whether what is sought to be achieved by the warrant could reasonably be achieved by other means.
- (8) An application for the issue of a warrant under this section may only be made on behalf of the head of an intelligence service by a person holding office under the Crown. 20
- (9) Nothing in subsection (2) or (4) prevents the Secretary of State from doing anything under this section for the purposes specified in section 2(2) of the European Communities Act 1972. 25

92 Power to issue warrants to intelligences services: the Scottish Ministers

- (1) The Scottish Ministers may, on an application made by or on behalf of the head of an intelligence service, issue a targeted equipment interference warrant if—
- (a) the warrant authorises interference only with equipment which is in Scotland at the time the warrant is issued or which the Scottish Ministers believe to be in Scotland at that time, 30
 - (b) the Scottish Ministers consider that the warrant is necessary for the purpose of preventing or detecting serious crime,
 - (c) the Scottish Ministers consider that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct, 35
 - (d) the Scottish Ministers consider that satisfactory arrangements made for the purposes of sections 112 and 113 (safeguards relating to disclosure etc.) are in force in relation to the warrant, and
 - (e) except where the Scottish Ministers consider that there is an urgent need to issue the warrant, the decision to issue the warrant has been approved by a Judicial Commissioner. 40
- (2) The Scottish Ministers may, on an application made by or on behalf of the head of an intelligence service, issue a targeted examination warrant if—
- (a) the warrant relates only to a person who is in Scotland, or whom the Scottish Ministers believe to be in Scotland, at the time of the issue of the warrant, 45

- (b) the Scottish Ministers consider that the warrant is necessary for the purpose of preventing or detecting serious crime,
 - (c) the Scottish Ministers consider that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct, 5
 - (d) the Scottish Ministers consider that the warrant is or may be necessary to authorise the selection of protected material in breach of the prohibition in section 170(4) (prohibition on seeking to identify communications of, or private information relating to, individuals in the British Islands), and 10
 - (e) except where the Scottish Ministers consider that there is an urgent need to issue the warrant, the decision to issue the warrant has been approved by a Judicial Commissioner.
- (3) The matters to be taken into account in considering whether the conditions in paragraphs (b) and (c) of subsection (1) are met include whether what is sought to be achieved by the warrant could reasonably be achieved by other means. 15
 - (4) An application for the issue of a warrant under this section may only be made on behalf of the head of an intelligence service by a person holding office under the Crown.
- 93 Power to issue warrants to the Chief of Defence Intelligence 20**
- (1) The Secretary of State may, on an application made by or on behalf of the Chief of Defence Intelligence, issue a targeted equipment interference warrant if—
 - (a) the Secretary of State considers that the warrant is necessary in the interests of national security,
 - (b) the Secretary of State considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct, 25
 - (c) the Secretary of State considers that satisfactory arrangements made for the purposes of section 112 and 113 (safeguards relating to disclosure etc.) are in force in relation to the warrant, and 30
 - (d) except where the Secretary of State considers that there is an urgent need to issue a warrant, the decision to issue it has been approved by a Judicial Commissioner.
 - (2) The matters to be taken into account in considering whether the conditions in paragraphs (a) and (b) of subsection (1) are met include whether what is sought to be achieved by the warrant could reasonably be achieved by other means. 35
 - (3) An application for the issue of a warrant under this section may only be made on behalf of the Chief of Defence Intelligence by a person holding office under the Crown.
- 94 Members of Parliament etc. 40**
- (1) This section applies where—
 - (a) an application is made to the Secretary of State for a targeted equipment interference warrant, and
 - (b) the purpose of the warrant is to obtain— 45
 - (i) communications sent by, or intended for, a person who is a member of a relevant legislature, or

- (ii) a member of a relevant legislature’s private information.
- (2) This section also applies where—
 - (a) an application is made to the Secretary of State for a targeted examination warrant, and
 - (b) the purpose of the warrant is to authorise the selection for examination of protected material which consists of—
 - (i) communications sent by, or intended for, a person who is a member of a relevant legislature, or
 - (ii) a member of a relevant legislature’s private information.
- (3) Before deciding whether to issue the warrant, the Secretary of State must consult the Prime Minister.
- (4) In this section “member of a relevant legislature” means—
 - (a) a member of either House of Parliament;
 - (b) a member of the Scottish Parliament;
 - (c) a member of the National Assembly for Wales;
 - (d) a member of the Northern Ireland Assembly;
 - (e) a member of the European Parliament elected for the United Kingdom.

- 95 Decision to issue warrants under sections 91 to 93 to be taken personally by Ministers**
 - (1) The decision to issue a warrant under section 91 or 93 must be taken personally by the Secretary of State.
 - (2) The decision to issue a warrant under section 92 must be taken personally by a member of the Scottish Government.
 - (3) Before a warrant under section 91, 92 or 93 is issued, it must be signed by the person who has taken the decision to issue it (subject to subsection (4)).
 - (4) If it is not reasonably practicable for a warrant to be signed by the person who has taken the decision to issue it, the warrant may be signed by a senior official designated by the Secretary of State or (as the case may be) the Scottish Ministers for that purpose.
 - (5) In such a case, the warrant must contain a statement that—
 - (a) it is not reasonably practicable for the warrant to be signed by the person who took the decision to issue it, and
 - (b) the Secretary of State or (as the case may be) the Scottish Ministers have personally and expressly authorised the issue of the warrant.

- 96 Power to issue warrants to law enforcement officers**
 - (1) A law enforcement chief described in Part 1 or 2 of the table in Schedule 6 may, on an application made by a person who is an appropriate law enforcement officer in relation to the chief, issue a targeted equipment interference warrant if—
 - (a) the law enforcement chief considers that the warrant is necessary for the purpose of preventing or detecting serious crime,
 - (b) the law enforcement chief considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct,

- (c) the law enforcement chief considers that satisfactory arrangements made for the purposes of sections 112 and 113 (safeguards relating to disclosure etc.) are in force in relation to the warrant, and
 - (d) except where the law enforcement chief considers that there is an urgent need to issue the warrant, the decision to issue it has been approved by a Judicial Commissioner. 5
- (2) A law enforcement chief described in Part 1 of the table in Schedule 6 may, on an application made by a person who is an appropriate law enforcement officer in relation to the chief, issue a targeted equipment interference warrant if—
 - (a) the law enforcement chief considers that the warrant is necessary for the purpose of preventing death or any injury or damage to a person’s physical or mental health or of mitigating any injury or damage to a person’s physical or mental health, 10
 - (b) the law enforcement chief considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct, 15
 - (c) the law enforcement chief considers that satisfactory arrangements made for the purposes of sections 112 and 113 (safeguards relating to disclosure etc.) are in force in relation to the warrant, and
 - (d) except where the law enforcement chief considers that there is an urgent need to issue the warrant, the decision to issue it has been approved by a Judicial Commissioner. 20
- (3) If it is not reasonably practicable for a law enforcement chief to consider an application under this section, an appropriate delegate may, in an urgent case, exercise the power to issue a targeted equipment interference warrant. 25
- (4) For the purposes of this section—
 - (a) a person is a law enforcement chief if the person is listed in the first column of the table in Schedule 6;
 - (b) a person is an appropriate delegate in relation to a law enforcement chief listed in the first column if the person is listed in the corresponding entry in the second column of that table; 30
 - (c) a person is an appropriate law enforcement officer in relation to a law enforcement chief listed in the first column if the person is listed in the corresponding entry in the third column of that table.
- (5) Where the law enforcement chief is the Chief Constable or the Deputy Chief Constable of the Police Service of Northern Ireland, the reference in subsection (1)(a) to the purpose of preventing or detecting serious crime includes a reference to the interests of national security. 35
- (6) A law enforcement chief who is an immigration officer may consider that the condition in subsection (1)(a) is satisfied only if the serious crime relates to an offence which is an immigration or nationality offence (whether or not it also relates to other offences). 40
- (7) A law enforcement chief who is an officer of Revenue and Customs may consider that the condition in subsection (1)(a) is satisfied only if the serious crime relates to an assigned matter within the meaning of section 1(1) of the Customs and Excise Management Act 1979. 45
- (8) A law enforcement chief who is a designated customs official may consider that the condition in subsection (1)(a) is satisfied only if the serious crime

- relates to a matter in respect of which a designated customs official has functions.
- (9) A law enforcement chief who is the chair of the Competition and Markets Authority may consider that the condition in subsection (1)(a) is satisfied only if the offence, or all of the offences, to which the serious crime relates are offences under section 188 of the Enterprise Act 2002. 5
 - (10) A law enforcement chief who is the Police Investigations and Review Commissioner may consider that the condition in subsection (1)(a) is satisfied only if the offence, or all of the offences, to which the serious crime relates are offences that are being investigated under section 33A(b)(i) of the Police, Public Order and Criminal Justice (Scotland) Act 2006. 10
 - (11) The matters to be taken into account in considering whether the conditions in paragraphs (a) and (b) of subsection (1) or (2) are met include whether what is sought to be achieved by the warrant could reasonably be achieved by other means. 15
 - (12) For the purpose of subsection (6), an offence is an immigration or nationality offence if conduct constituting the offence –
 - (a) relates to the entitlement of one or more persons who are not nationals of the United Kingdom to enter, transit across, or be in, the United Kingdom (including conduct which relates to conditions or other controls on any such entitlement), or 20
 - (b) is undertaken for the purposes of or otherwise in relation to –
 - (i) the British Nationality Act 1981;
 - (ii) the Hong Kong Act 1985;
 - (iii) the Hong Kong (War Wives and Widows) Act 1996; 25
 - (iv) the British Nationality (Hong Kong) Act 1997;
 - (v) the British Overseas Territories Act 2002;
 - (vi) an instrument made under any of those Acts.
 - (13) In this section –
 - “designated customs official” has the same meaning as in Part 1 of the Borders, Citizenship and Immigration Act 2009 (see section 14(6) of that Act); 30
 - “immigration officer” means a person appointed as an immigration officer under paragraph 1 of Schedule 2 to the Immigration Act 1971.

Approval of warrants by Judicial Commissioners 35

97 Approval of warrants by Judicial Commissioners

- (1) In deciding whether to approve a person’s decision to issue a warrant under this Part, a Judicial Commissioner must review the person’s conclusions as to the following matters –
 - (a) whether the warrant is necessary on any relevant grounds (see subsection (3)), and 40
 - (b) whether the conduct which would be authorised by the warrant is proportionate to what is sought to be achieved by that conduct.

- (2) In doing so, the Judicial Commissioner must apply the same principles as would be applied by a court on an application for judicial review.
- (3) In subsection (1)(a), “relevant grounds” means—
 - (a) in the case of a warrant to be issued under section 91, grounds falling within section 91(5); 5
 - (b) in the case of a warrant to be issued under section 92, the purpose of preventing or detecting serious crime;
 - (c) in the case of a warrant to be issued under section 93, the interests of national security;
 - (d) in the case of a warrant to be issued under section 96(1), the purpose mentioned in section 96(1)(a); 10
 - (e) in the case of a warrant to be issued under section 96(2), the purpose mentioned in section 96(2)(a).
- (4) Where a Judicial Commissioner refuses to approve a person’s decision to issue a warrant under this Part, the Judicial Commissioner must give the person written reasons for the refusal. 15
- (5) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve a person’s decision to issue a warrant under this Part, the person may ask the Investigatory Powers Commissioner to decide whether to approve the decision to issue the warrant. 20

98 Approval of warrants issued in urgent cases

- (1) This section applies where—
 - (a) a warrant under this Part is issued without the approval of a Judicial Commissioner, and
 - (b) the person who issued the warrant considered that there was an urgent need to issue it. 25
- (2) The person who issued the warrant must inform a Judicial Commissioner that it has been issued.
- (3) The Judicial Commissioner must, before the end of the relevant period—
 - (a) decide whether to approve the decision to issue the warrant, and 30
 - (b) notify the person of the Judicial Commissioner’s decision.

“The relevant period” means the period ending with the third working day after the day on which the warrant was issued.
- (4) If a Judicial Commissioner refuses to approve the decision to issue a warrant, the warrant— 35
 - (a) ceases to have effect (unless already cancelled), and
 - (b) may not be renewed.
- (5) Section 99 contains further provision about what happens if a Judicial Commissioner refuses to approve the decision to issue a warrant.

99 Failure to approve warrant issued in urgent case 40

- (1) This section applies where under section 98(3) a Judicial Commissioner refuses to approve the decision to issue a warrant.

- (2) The person to whom the warrant was addressed must, so far as is reasonably practicable, secure that anything in the process of being done under the warrant stops as soon as possible.
- (3) Where the refusal relates to a targeted equipment interference warrant, the Judicial Commissioner may – 5
- (a) authorise further interference with equipment for the purpose of enabling the person to whom the warrant is addressed to secure that anything in the process of being done under the warrant stops as soon as possible;
 - (b) direct that any of the material obtained under the warrant is destroyed; 10
 - (c) impose conditions as to the use or retention of any of that material.
- (4) Where the refusal relates to a targeted examination warrant, the Judicial Commissioner may impose conditions as to the use of any protected material selected for examination under the warrant.
- (5) The Judicial Commissioner – 15
- (a) may require an affected party to make representations about how the Judicial Commissioner should exercise any function under subsection (3) or (4), and
 - (b) must have regard to any such representations made by an affected party (whether or not as a result of a requirement imposed under paragraph (a)). 20
- (6) Each of the following is an “affected party” for the purposes of subsection (5) –
- (a) the person who decided to issue the warrant;
 - (b) the person to whom the warrant was addressed.
- (7) The person who decided to issue the warrant may ask the Investigatory Powers Commissioner to review a decision made by any other Judicial Commissioner under subsection (3) or (4). 25
- (8) On a review under subsection (7), the Investigatory Powers Commissioner may – 30
- (a) confirm the Judicial Commissioner’s decision, or
 - (b) make a fresh determination.
- (9) Nothing in this section or section 98 affects the lawfulness of – 35
- (a) anything done under the warrant before it ceases to have effect;
 - (b) if anything is in the process of being done under the warrant when it ceases to have effect –
 - (i) anything done before that thing could be stopped, or
 - (ii) anything done that it is not reasonably practicable to stop.

*Additional safeguards***100 Items subject to legal privilege**

- (1) Subsections (2) and (3) apply if – 40
- (a) an application is made for a warrant under this Part, and
 - (b) the purpose, or one of the purposes, of the warrant is –

- (i) in the case of a targeted equipment interference warrant, to authorise or require interference with equipment for the purpose of obtaining items subject to legal privilege, or
 - (ii) in the case of a targeted examination warrant, to authorise the selection of such items for examination. 5
- (2) The application must contain a statement that the purpose, or one of the purposes, of the warrant is to authorise or require interference with equipment for the purpose of obtaining items subject to legal privilege or (in the case of a targeted examination warrant) the selection for examination of items subject to legal privilege. 10
- (3) The person to whom the application is made may issue the warrant only if the person considers –
 - (a) that there are exceptional and compelling circumstances which make it necessary to authorise or require interference with equipment for the purpose of obtaining items subject to legal privilege or (in the case of a targeted examination warrant) the selection for examination of items subject to legal privilege, and 15
 - (b) that the arrangements made for the purposes of section 112 or (as the case may be) section 168 (safeguards relating to retention and disclosure of material) include specific arrangements for the handling, retention, use and destruction of such items. 20
- (4) Subsections (5) and (6) apply if –
 - (a) an application is made for a warrant under this Part,
 - (b) the applicant considers that the relevant material is likely to include items subject to legal privilege, and 25
 - (c) subsections (2) and (3) do not apply.
- (5) The application must contain –
 - (a) a statement that the applicant considers that the relevant material is likely to include items subject to legal privilege, and
 - (b) an assessment of how likely it is that the relevant material will include such items. 30
- (6) The person to whom the application is made may issue the warrant only if the person considers that the arrangements made for the purposes of section 112 or (as the case may be) section 168 include specific arrangements for the handling, retention, use and destruction of items subject to legal privilege. 35
- (7) In this section, “relevant material” means –
 - (a) in relation to a targeted equipment interference warrant, any material the obtaining of which is authorised or required under the warrant;
 - (b) in relation to a targeted examination warrant, any protected material which the warrant authorises to be selected for examination. 40

Further provision about warrants

101 Requirements which must be met by warrants

- (1) A warrant under this Part must contain a provision stating whether it is a targeted equipment interference warrant or a targeted examination warrant.
- (2) A warrant under this Part must be addressed – 45

- (a) in the case of a warrant issued under section 91 or 92, to the head of the intelligence service by whom or on whose behalf the application for the warrant was made;
 - (b) in the case of a warrant issued under section 93, to the Chief of Defence Intelligence; 5
 - (c) in the case of a warrant issued under section 96 by a law enforcement chief (or by an appropriate delegate in relation to a law enforcement chief), to a person who—
 - (i) is an appropriate law enforcement officer in relation to the law enforcement chief, and 10
 - (ii) is named or described in the warrant.
- (3) In the case of a targeted equipment interference warrant which relates to a matter described in the first column of the Table below, the warrant must include the details specified in the second column.

<i>Matter</i>	<i>Details to be included in the warrant</i>	
Equipment belonging to, used by or in the possession of a particular person or organisation	The name of the person or organisation or a description of the person or organisation	15
Equipment belonging to, used by or in the possession of persons who form a group which shares a common purpose or who carry on, or may carry on, a particular activity	A description of the purpose or activity and the name of, or a description of, as many of the persons as it is reasonably practicable to name or describe	20
Equipment used by or in the possession of more than one person or organisation, where the interference is for the purpose of a single investigation or operation	A description of the nature of the investigation or operation and the name of, or a description of, as many of the persons or organisations as it is reasonably practicable to name or describe	25
Equipment in a particular location	A description of the location	30
Equipment in more than one location, where the interference is for the purpose of a single investigation or operation	A description of the nature of the investigation or operation and a description of as many of the locations as it is reasonably practicable to describe	35
Equipment in more than one location, where the interference is for the purpose of a single investigation or operation	A description of the nature of the investigation or operation and a description of as many of the locations as it is reasonably practicable to describe	40

<i>Matter</i>	<i>Details to be included in the warrant</i>	
Equipment which is being, or may be used, for the purposes of a particular activity or activities of a particular description	A description of the particular activity or activities	5
Equipment which is being, or may be used, to test, maintain or develop capabilities relating to interference with equipment	A description of the nature of the testing, maintenance or development of capabilities	10
Equipment which is being, or may be used, for the training of persons who carry out, or are likely to carry out, interference with equipment	A description of the nature of the training	15
(4) A targeted equipment interference warrant must also describe – (a) the type of equipment which is to be interfered with, and (b) the conduct which the person to whom the warrant is addressed is authorised to take.		20
(5) In the case of a targeted examination warrant which relates to a matter described in the first column of the Table below, the warrant must include the details specified in the second column.		25

<i>Matter</i>	<i>Details to be included in the warrant</i>	
A particular person or organisation	The name of the person or organisation or a description of the person or organisation	30
A group of persons who share a common purpose or who carry on or may carry on a particular activity	A description of the purpose or activity and the name of, or a description of, as many of the persons as it is reasonably practicable to name or describe	35
More than one person or organisation, where the interference is for the purpose of a single investigation or operation	A description of the nature of the investigation or operation and the name of, or a description of, as many of the persons or organisations as it is reasonably practicable to name or describe	40

<i>Matter</i>	<i>Details to be included in the warrant</i>	
The testing, maintenance or development of capabilities relating to the selection or protected material for examination	A description of the nature of the testing, maintenance or development of capabilities	5
The training of persons who carry out, or are likely to carry out, the selection of protected material for examination	A description of the nature of the training	10

102 Duration of warrants

- (1) A warrant issued under this Part ceases to have effect at the end of the relevant period (see subsection (2)), unless – 15
 - (a) it is renewed before the end of that period (see section 103), or
 - (b) it is cancelled or otherwise ceases to have effect before the end of that period (see sections 98 and 108).

- (2) In this section, “the relevant period” – 20
 - (a) in the case of an urgent warrant which has not been renewed, means the period ending with the fifth working day after the day on which the warrant was issued;
 - (b) in any other case, means the period of 6 months beginning with – 25
 - (i) the day on which the warrant was issued, or
 - (ii) in the case of a warrant which has been renewed, the day after the day at the end of which the warrant would have ceased to have effect if it had not been renewed.

- (3) For the purposes of subsection (2)(a), a warrant is an “urgent warrant” if – 30
 - (a) the warrant was issued without the approval of a Judicial Commissioner, and
 - (b) the person who decided to issue the warrant considered that there was an urgent need to issue it.

103 Renewal of warrants

- (1) If the renewal conditions are met, a warrant issued under this Part may be renewed, at any time before the end of the relevant period, by an instrument issued by the appropriate person (see subsection (3)). 35

- (2) The renewal conditions are – 40
 - (a) that the appropriate person considers that the warrant continues to be necessary on any relevant grounds,
 - (b) that the appropriate person considers that the conduct that would be authorised by the warrant continues to be proportionate to what is sought to be achieved by that conduct,
 - (c) that, in the case of a targeted examination warrant, the appropriate person considers that the warrant continues to be necessary to

- authorise the selection of protected material for examination in breach of the prohibition in section 170(4), and
- (d) that the decision to renew the warrant has been approved by a Judicial Commissioner.
- (3) The appropriate person is— 5
- (a) in the case of a warrant issued under section 91 or 93, the Secretary of State;
- (b) in the case of a warrant issued under section 92, a member of the Scottish Government;
- (c) in the case of a warrant issued under section 96 by a law enforcement chief or by an appropriate delegate in relation to the law enforcement chief, either— 10
- (i) the law enforcement chief, or
- (ii) if the warrant was issued by an appropriate delegate, that person. 15
- (4) In subsection (2)(a), “relevant grounds” means—
- (a) in the case of a warrant issued under section 91, grounds falling within section 91(5),
- (b) in the case of a warrant issued under section 92, the purpose of preventing or detecting serious crime, 20
- (c) in the case of a warrant issued under section 93, the interests of national security,
- (d) in the case of a warrant to be issued under section 96(1), the purpose mentioned in section 96(1)(a), or
- (e) in the case of a warrant to be issued under section 96(2), the purpose mentioned in section 96(2)(a). 25
- (5) The decision to renew a warrant issued under section 91 or 93 must be taken personally by the Secretary of State, and the instrument renewing the warrant must be signed by the Secretary of State.
- (6) The decision to renew a warrant issued under section 92 must be taken personally by a member of the Scottish Government, and the instrument renewing the warrant must be signed by the person who took that decision. 30
- (7) The instrument renewing a warrant issued under section 96 must be signed by the person who renews it.
- (8) Section 94 (Members of Parliament etc.) applies in relation to a decision to renew a warrant under this Part issued by the Secretary of State as it applies in relation to a decision to issue such a warrant. 35
- (9) Section 97 (approval of warrants by Judicial Commissioners) applies in relation to a decision to renew a warrant under this Part as it applies in relation to a decision to issue such a warrant (and accordingly any reference in that section to the person who decided to issue the warrant is to be read as a reference to the person who decided to renew it). 40
- (10) Section 100 (items subject to legal privilege) applies in relation to a decision to renew a warrant under this Part as it applies in relation to a decision to issue such a warrant. 45
- (11) In this section, “relevant period” has the same meaning as in section 102.

104 Modification of warrants issued by the Secretary of State or Scottish Ministers

- (1) The provisions of a warrant issued under section 91, 92 or 93 may be modified at any time by an instrument issued by the person making the modification.
- (2) The only modifications which may be made under this section are – 5
- (a) adding to the matters to which the warrant relates (see sections 90(1) and (2)), by including the details required in relation to that matter by section 101(3) or (5);
 - (b) removing a matter to which the warrant relates;
 - (c) adding (in relation to a matter to which the warrant relates) a name or description to the names or descriptions included in the warrant in accordance with section 101(3) or (5); 10
 - (d) varying or removing (in relation to a matter to which the warrant relates), a name or description included in the warrant in accordance with section 101(3) or (5); 15
 - (e) adding to the descriptions of types of equipment included in the warrant in accordance with section 101(4)(a);
 - (f) varying or removing a description of a type of equipment included in the warrant in accordance with section 101(4)(a).
- (3) The decision to modify the provisions of a warrant must be taken personally by the person making the modification, and the instrument making the modification must be signed by that person. 20
- (4) A modification may be made only if the person making the modification considers that –
- (a) the warrant as modified continues to be necessary on any relevant grounds (see subsection (5)), and 25
 - (b) the conduct authorised by the warrant as so modified is proportionate to what is sought to be achieved by that conduct.
- (5) In subsection (4)(a), “relevant grounds” means –
- (a) in the case of a warrant issued under section 91, grounds falling within section 91(5); 30
 - (b) in the case of a warrant issued under section 92, the purpose of preventing or detecting serious crime;
 - (c) in the case of a warrant issued under section 93, the interests of national security. 35
- (6) The persons who may make modifications under this section of a warrant are (subject to subsection (7)) –
- (a) in the case of a warrant issued by the Secretary of State under section 91 or 93 – 40
 - (i) the Secretary of State,
 - (ii) a senior official acting on behalf of the Secretary of State,
 - (b) in the case of a warrant issued by the Scottish Ministers under section 92 –
 - (i) a member of the Scottish Government, or 45
 - (ii) a senior official acting on behalf of the Scottish Ministers.
- (7) Any of the following persons may also make modifications under this section of a warrant, but only where the person considers that there is an urgent need to make the modification –

- (a) the person to whom the warrant is addressed;
- (b) a person who holds a senior position in the same public authority as the person mentioned in paragraph (a).
- Section 105 contains provision about the approval of modifications made in urgent cases. 5
- (8) For the purposes of subsection (7)(b), a person holds a senior position in a public authority if—
- (a) in the case of any of the intelligence services—
- (i) the person is a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty’s Diplomatic Service, or 10
- (ii) the person holds a position in the intelligence service of equivalent seniority to such a person;
- (b) in the case of the Ministry of Defence—
- (i) the person is a member of the Senior Civil Service, or 15
- (ii) the person is of or above the rank of brigadier, commodore or air commodore.
- (9) Sections 94 (Members of Parliament etc.) applies in relation to a decision to make a modification of a warrant issued under section 91 or 93 which is of a kind described in subsection (2)(a), (c) or (e) as it applies in relation to a decision to issue such a warrant; and accordingly where that section applies only the Secretary of State may make the modification. 20
- (10) Section 100 (items subject to legal privilege) applies in relation to a decision to make a modification of a warrant issued under section 91, 92 or 93 which is of a kind described in subsection (2)(a), (c) or (e) as it applies in relation to a decision to issue such a warrant. 25
- (11) Where a senior official has made a modification of a warrant issued under section 91 or 93, the Secretary of State must be notified personally of the modification and the reasons for making it.
- (12) Where a senior official has made a modification of a warrant issued under section 92, a member of the Scottish Government must be notified personally of the modification and the reasons for making it. 30
- (13) Nothing in this section applies in relation to modifying the provisions of a warrant in a way which does not affect the conduct authorised or required by it. 35
- 105 Approval of modifications under section 104 made in urgent cases**
- (1) This section applies where a person makes a modification of a warrant by virtue of section 104(7).
- (2) The person who made the modification must inform a designated senior official that it has been made. 40
- (3) In this section, “designated senior official” means a senior official who has been designated by the Secretary of State or (in the case of warrants issued by the Scottish Ministers) the Scottish Ministers for the purposes of this section.
- (4) In addition, the Secretary of State or (in the case of a warrant issued by the Scottish Ministers) a member of the Scottish Government must be notified personally of the modification and the reasons for making it. 45

- (5) The designated senior official must, before the end of the relevant period –
- (a) decide whether to approve the decision to make the modification, and
 - (b) notify the person of the senior official’s decision.
- “The relevant period” means the period ending with the fifth working day after the day on which the modification was made. 5
- (6) If the designated senior official refuses to approve the decision to make the modification –
- (a) the Secretary of State or (in the case of a warrant issued by the Scottish Ministers) a member of the Scottish Government must be notified personally of the refusal, 10
 - (b) the warrant (unless it no longer has effect) has effect as if the modification had not been made, and
 - (c) the person to whom the warrant is addressed must, so far as is reasonably practicable, secure that anything in the process of being done under the warrant by virtue of that modification stops as soon as possible. 15
- (7) In a case where a designated senior official refuses to approve a decision to make a modification of a targeted equipment interference warrant, the designated senior official may authorise further interference with equipment for the purpose of enabling the person to whom the warrant is addressed to secure that anything in the process of being done under the warrant by virtue of the modification stops as soon as possible. 20
- (8) If the designated senior official authorises further interference with equipment under subsection (7), the Secretary of State or (in the case of a warrant issued by the Scottish Ministers) a member of the Scottish Government must be notified personally of the authorisation. 25
- (9) Nothing in this section affects the lawfulness of –
- (a) anything done under the warrant by virtue of the modification before the modification ceases to have effect;
 - (b) if anything is in the process of being done under the warrant by virtue of the modification when the modification ceases to have effect – 30
 - (i) anything done before that thing could be stopped, or
 - (ii) anything done which it is not reasonably practicable to stop.

106 Modification of warrants issued by law enforcement chiefs

- (1) The provisions of a warrant issued under section 96 by a law enforcement chief, or by an appropriate delegate in relation to that chief, may be modified at any time by – 35
- (a) the law enforcement chief, or
 - (b) if the warrant was issued by an appropriate delegate, by that person.
- (2) The only modifications which may be made under this section are – 40
- (a) adding to the matters to which the warrant relates (see sections 90(1) and (2)), by including the details required in relation to that matter by section 101(3) or (5);
 - (b) removing a matter to which the warrant relates;
 - (c) adding (in relation to a matter to which the warrant relates) a name or description to the names or descriptions included in the warrant in accordance with section 101(3) or (5); 45

- (d) varying or removing (in relation to a matter to which the warrant relates) a name or description included in the warrant in accordance with section 101(3) or (5);
 - (e) adding to the descriptions of types of equipment included in the warrant in accordance with section 101(4)(a); 5
 - (f) varying or removing a description of a type of equipment included in the warrant in accordance with section 101(4)(a).
- (3) A modification may be made only if—
- (a) the person making the modification considers that—
 - (i) the warrant as modified continues to be necessary on any relevant grounds (see subsection (4)), and 10
 - (ii) the conduct authorised by the warrant as so modified is proportionate to what is sought to be achieved by that conduct, and
 - (b) except where the person making the modification considers that there is an urgent need to make it, the decision to make the modification has been approved by a Judicial Commissioner. 15
- (4) In subsection (3)(a), “relevant grounds” means—
- (a) in the case of a warrant to be issued under section 96(1), the purpose mentioned in section 96(1)(a); 20
 - (b) in the case of a warrant to be issued under section 96(2), the purpose mentioned in section 96(2)(a).
- (5) The decision to make any modification must be taken personally by the person making the modification, and the instrument making the modification must be signed by that person. 25
- (6) Section 97 (approval of warrants by Judicial Commissioners) applies in relation to a decision to make a modification of a warrant issued under section 96 as it applies in relation to a decision to issue such a warrant, but as if—
- (a) the references in subsection (1)(a) and (b) of that section to the warrant were references to the warrant as modified, and 30
 - (b) any reference to the person who decided to issue the warrant were a reference to the person who decided to make the modification.
- (7) Section 100 (items subject to legal privilege) applies in relation to a decision to make a modification of a warrant issued under section 96 which is of a kind described in subsection (2)(a), (c) or (e) as it applies in relation to a decision to issue such a warrant. 35
- (8) Nothing in this section applies in relation to modifying the provisions of a warrant in a way which does not affect the conduct authorised or required by it.
- 107 Approval of modifications under section 106 in urgent cases 40**
- (1) This section applies where—
- (a) a modification is made under section 106 without the approval of a Judicial Commissioner, and
 - (b) the person who made the modification considered that there was an urgent need to make it. 45

- (2) The person who made the modification must inform a Judicial Commissioner that it has been made.
- (3) The Judicial Commissioner must, before the end of the relevant period –
 - (a) decide whether to approve the decision to make the modification, and
 - (b) notify the person of the Judicial Commissioner’s decision. 5

“The relevant period” means the period ending with the fifth working day after the day on which the modification was made.
- (4) If the Judicial Commissioner refuses to approve the decision to make the modification –
 - (a) the person who issued the warrant must be notified of the refusal, 10
 - (b) the warrant (unless it no longer has effect) has effect as if the modification had not been made, and
 - (c) the person to whom the warrant is addressed must, so far as is reasonably practicable, secure that anything in the process of being done under the warrant by virtue of that modification stops as soon as possible. 15
- (5) In a case where a Judicial Commissioner refuses to approve a decision to make a modification of a targeted equipment interference warrant, the Judicial Commissioner may authorise further interference with equipment for the purpose of enabling the person to whom the warrant is addressed to secure that anything in the process of being done under the warrant by virtue of the modification stops as soon as possible. 20
- (6) If the Judicial Commissioner authorises further interference with equipment under subsection (5), the person who issued the warrant must be informed of the authorisation. 25
- (7) Nothing in this section affects the lawfulness of –
 - (a) anything done under the warrant by virtue of the modification before the modification ceases to have effect;
 - (b) if anything is in the process of being done under the warrant by virtue of the modification when the modification ceases to have effect – 30
 - (i) anything done before that thing could be stopped, or
 - (ii) anything done which it is not reasonably practicable to stop.

108 Cancellation of warrants

- (1) Any of the appropriate persons may cancel a warrant issued under this Part at any time. 35
- (2) If any of the appropriate persons considers that –
 - (a) a warrant issued under this Part is no longer necessary on any relevant grounds, or
 - (b) the conduct authorised by a warrant issued under this Part is no longer proportionate to what is sought to be achieved by the conduct, 40

the person must cancel the warrant.
- (3) In subsection (2)(a), “relevant grounds” means –
 - (a) in the case of a warrant issued under section 91, grounds falling within section 91(5);
 - (b) in the case of a warrant issued under section 92, the purpose of preventing or detecting serious crime; 45

- (c) in the case of a warrant issued under section 93, the interests of national security;
 - (d) in the case of a warrant to be issued under section 96(1), the purpose mentioned in section 96(1)(a);
 - (e) in the case of a warrant to be issued under section 96(2), the purpose mentioned in section 96(2)(a). 5
- (4) For the purposes of this section, “the appropriate persons” are –
- (a) in the case of a warrant issued by the Secretary of State under section 91 or 93, the Secretary of State or a senior official acting on behalf of the Secretary of State; 10
 - (b) in the case of a warrant issued by the Scottish Ministers under section 92, a member of the Scottish Government or a senior official acting on behalf of the Scottish Ministers;
 - (c) in the case of a warrant issued under section 96 by a law enforcement chief or by an appropriate delegate in relation to the law enforcement chief, either – 15
 - (i) the law enforcement chief, or
 - (ii) if the warrant was issued by an appropriate delegate, that person.
- (5) Where a warrant is cancelled under this section, the person to whom the warrant is addressed must, so far as is reasonably practicable, secure that anything in the process of being done under the warrant stops as soon as possible. 20
- (6) A warrant that has been cancelled under this section may not be renewed.

Implementation of warrants 25

109 Implementation of warrants

- (1) In giving effect to a targeted equipment interference warrant, the person to whom it is addressed (“the implementing authority”) may (in addition to acting alone) act through, or together with, such other persons as the implementing authority may require (whether under subsection (2) or otherwise) to provide the authority with assistance in giving effect to the warrant. 30
- (2) For the purpose of requiring any person to provide assistance in relation to a targeted equipment interference warrant, the implementing authority may – 35
- (a) serve a copy of the warrant on any person whom the implementing authority considers may be able to provide such assistance, or
 - (b) make arrangements for the service of a copy of the warrant on any such person.
- (3) A copy of a warrant may be served under subsection (2) on a person outside the United Kingdom for the purpose of requiring the person to provide such assistance in the form of conduct outside the United Kingdom. 40
- (4) For the purposes of this Act, the provision of assistance in giving effect to a targeted equipment interference warrant includes any disclosure to the implementing authority, or to persons acting on that person’s behalf, of material obtained under the warrant. 45

- (5) The references in subsections (2) and (3) and sections 110 and 111 to the service of a copy of a warrant include—
 - (a) the service of a copy of one or more schedules contained in the warrant with the omission of the remainder of the warrant, and
 - (b) the service of a copy of the warrant with the omission of any schedule contained in it. 5

110 Service of warrants outside the United Kingdom

- (1) This section applies to the service of warrants under section 109(2) on a person outside the United Kingdom.
- (2) A copy of a warrant may be served on a person outside the United Kingdom in any of the following ways (as well as by electronic or other means of service)— 10
 - (a) by serving it at the person’s principal office within the United Kingdom or, if the person has no such office in the United Kingdom, at any place in the United Kingdom where the person carries on business or conducts activities; 15
 - (b) if the person has specified an address in the United Kingdom as one at which the person, or someone on the person’s behalf, will accept service of documents of the same description as a copy of a warrant, by serving it at that address;
 - (c) by making it available for inspection (whether to the person or to someone acting on the person’s behalf) at a place in the United Kingdom (but this is subject to subsection (3)). 20
- (3) A copy of a warrant may be served on a person outside the United Kingdom in the way mentioned in subsection (2)(c) only if—
 - (a) it is not reasonably practicable for a copy to be served by any other means (whether as mentioned in subsection (2)(a) or (b) or otherwise), and 25
 - (b) the implementing authority takes such steps as it considers appropriate for the purpose of bringing the contents of the warrant, and the availability of a copy for inspection, to the attention of the person. 30
- (4) The steps mentioned in subsection (3)(b) must be taken as soon as reasonably practicable after the copy of the warrant is made available for inspection.
- (5) In this section, “implementing authority” has the same meaning as in section 109.

111 Duty of telecommunications operators to assist with implementation 35

- (1) A telecommunications operator that has been served with a copy of a targeted equipment interference warrant issued by the Secretary of State under section 91 or 93, or by the Scottish Ministers under section 92, must take all steps for giving effect to the warrant which are notified to the telecommunications operator by or on behalf of the person to whom the warrant is addressed. 40
- (2) A telecommunications operator that has been served with a copy of a targeted equipment interference warrant issued under section 96 and addressed to a law enforcement officer mentioned in subsection (3) must take all steps for giving effect to the warrant which—

- (a) were approved by the Secretary of State or, in the case of a warrant addressed to a constable of the Police Service of Scotland, by the Scottish Ministers, before the warrant was served, and
 - (b) are notified to the telecommunications operator by or on behalf of the law enforcement officer. 5
- (3) The law enforcement officers mentioned in this subsection are –
- (a) a National Crime Agency officer;
 - (b) an officer of Revenue and Customs;
 - (c) a constable of the Police Service of Scotland;
 - (d) a member of the Police Service of Northern Ireland; 10
 - (e) a member of the metropolitan police force.
- (4) The Secretary of State or the Scottish Ministers may give approval for the purposes of subsection (2)(a) if the Secretary of State or (as the case may be) the Scottish Ministers consider that –
- (a) it is necessary for the telecommunications operator to be required to take the steps, and 15
 - (b) the steps are proportionate to what is sought to be achieved by them.
- (5) A telecommunications operator is not required to take any steps which is not reasonably practicable for the telecommunications operator to take.
- (6) Where obligations have been imposed on a telecommunications operator (“P”) under section 217 (maintenance of technical capability), for the purposes of subsection (5) the steps which it is reasonably practicable for P to take include every step which it would have been reasonably practicable for P to take if P had complied with all of those obligations. 20
- (7) The duty imposed by subsection (1) or (2) is enforceable against a person in the United Kingdom by civil proceedings by the Secretary of State for an injunction, or for specific performance of a statutory duty under section 45 of the Court of Session Act 1988, or for any other appropriate relief. 25

Supplementary provision

- 112 Safeguards relating to retention and disclosure of material** 30
- (1) The issuing authority must ensure, in relation to every targeted equipment interference warrant issued by that authority, that arrangements are in force for securing that the requirements of subsections (2) and (5) are met in relation to the material obtained under the warrant. 35
 This is subject to subsection (10).
- (2) The requirements of this subsection are met in relation to the material obtained under a warrant if each of the following is limited to the minimum that is necessary for the authorised purposes (see subsection (3)) –
- (a) the number of persons to whom any of the material is disclosed or otherwise made available; 40
 - (b) the extent to which any of the material is disclosed or otherwise made available;
 - (c) the extent to which any of the material is copied;
 - (d) the number of copies that are made.

- (3) For the purposes of subsection (2), something is necessary for the authorised purposes if, and only if—
 - (a) it is, or is likely to become, necessary on any relevant grounds (see subsection (7)),
 - (b) it is necessary for facilitating the carrying out of any functions under this Act of the Secretary of State, the Scottish Ministers or the person to whom the warrant is addressed, 5
 - (c) it is necessary for facilitating the carrying out of any functions of the Judicial Commissioners or of the Investigatory Powers Tribunal under or in relation to this Act, 10
 - (d) it is necessary for the purpose of legal proceedings, or
 - (e) it is necessary for the performance of the functions of any person by or under any enactment.

- (4) The arrangements for the time being in force under this section for securing that the requirements of subsection (2) are met in relation to the material obtained under the warrant must include arrangements for securing that every copy made of any of that material is stored, for so long as it is retained, in a secure manner. 15

- (5) The requirements of this subsection are met in relation to the material obtained under a warrant if every copy made of any of that material (if not destroyed earlier) is destroyed as soon as there are no longer any grounds for retaining it (see subsection (6)). 20

- (6) For the purposes of subsection (5), there are no longer any grounds for retaining a copy of any material if, and only if—
 - (a) its retention is not necessary, or not likely to become necessary, on any relevant grounds (see subsection (7)), and 25
 - (b) its retention is not necessary for any of the purposes mentioned in paragraphs (b) to (e) of subsection (3) above.

- (7) In subsections (3) and (6), “relevant grounds” means—
 - (a) in relation to a warrant issued under section 91, grounds falling within section 91(5); 30
 - (b) in relation to a warrant issued under section 92, the purpose of preventing or detecting serious crime;
 - (c) in relation to a warrant issued under section 93, the interests of national security; 35
 - (d) in the case of a warrant issued under section 96(1), the purpose mentioned in section 96(1)(a);
 - (e) in the case of a warrant issued under section 96(2), the purpose mentioned in section 96(2)(a).

- (8) Where an item subject to legal privilege is retained following its examination under a warrant issued under this Part, the person retaining it must inform the Investigatory Powers Commissioner as soon as is reasonably practicable. 40

- (9) Subsection (10) applies if—
 - (a) any material obtained under the warrant has been handed over to any overseas authorities, or 45
 - (b) a copy of any such material has been given to any overseas authorities.

- (10) To the extent that the requirements of subsections (2) and (5) relate to any of the material mentioned in subsection (9)(a), or to the copy mentioned in

subsection (9)(b), the arrangements made for the purpose of this section are not required to secure that those requirements are met (see instead section 113).

(11) In this section –

“copy”, in relation to material obtained under a warrant, means any of the following (whether or not in documentary form) – 5

- (a) any copy, extract or summary of the material which identifies the material as having been obtained under the warrant, and
- (b) any record which is a record of the identities of persons who owned, used or were in possession of the equipment which was interfered with to obtain that material, 10

and “copied” is to be read accordingly;

“the issuing authority” means –

- (a) in the case of a warrant issued under section 91 or 93, the Secretary of State;
- (b) in the case of a warrant issued under section 92, the Scottish Ministers; 15
- (c) in the case of a warrant issued under section 96, the law enforcement chief who issued the warrant (or on whose behalf it was issued);

“overseas authorities” means authorities of a country or territory outside the United Kingdom. 20

113 Safeguards relating to disclosure of material or data overseas

(1) The issuing authority must ensure, in relation to every targeted equipment interference warrant, that arrangements are in force for securing that –

- (a) any material obtained under the warrant is handed over to overseas authorities only if the requirements of subsection (2) are met, and 25
- (b) copies of any such material are given to overseas authorities only if those requirements are met.

(2) The requirements of this subsection are met in the case of a warrant if it appears to the issuing authority that requirements corresponding to the requirements of section 112(2) and (5) (“the relevant requirements”) will apply, to such extent (if any) as the issuing authority considers appropriate, in relation to any of the material which is handed over, or any copy of which is given, to the authorities in question. 30

(3) In this section – 35

“copy” has the same meaning as in section 112;
 “issuing authority” also has the same meaning as in that section;
 “overseas authorities” means authorities of a country or territory outside the United Kingdom.

114 Duty not to make unauthorised disclosures 40

(1) A person to whom this section applies must not make an unauthorised disclosure to another person.

(2) A person makes an unauthorised disclosure for the purposes of this section if –
 (a) the person discloses any of the matters within subsection (4) in relation to a warrant under this Part, and 45

- (b) the disclosure is not an excepted disclosure (see section 115).
- (3) This section applies to the following persons –
 - (a) any person who may apply for a warrant under this Part;
 - (b) any person holding office under the Crown;
 - (c) any person employed by, or for the purposes of, a police force; 5
 - (d) any telecommunications operator;
 - (e) any person employed or engaged for the purposes of any business of a telecommunications operator;
 - (f) any person to whom any of the matters within subsection (4) have been disclosed in relation to a warrant under this Part. 10
- (4) The matters referred to in subsection (2)(a) are –
 - (a) the existence or contents of the warrant;
 - (b) the details of the issue of the warrant or of any renewal or modification of the warrant;
 - (c) the existence or contents of any requirement to provide assistance in giving effect to the warrant; 15
 - (d) the steps taken in pursuance of the warrant or of any such requirement;
 - (e) any of the material obtained under the warrant in a form which identifies it as having been obtained under a warrant under this Part.
- 115 Section 114: meaning of “excepted” disclosure 20**
 - (1) For the purposes of section 114, a disclosure made in relation to a warrant is an authorised disclosure if it falls within any of the Heads set out in –
 - (a) subsection (2) (disclosures authorised by warrant etc.);
 - (b) subsection (3) (oversight bodies);
 - (c) subsection (4) (legal proceedings); 25
 - (d) subsection (6) (disclosures of a general nature).
 - (2) Head 1 is –
 - (a) a disclosure authorised by the warrant;
 - (b) a disclosure authorised by the person to whom the warrant is or was addressed or under any arrangements made by that person for the purposes of this section; 30
 - (c) a disclosure authorised by the terms of any requirement to provide assistance in giving effect to the warrant (including any requirement for disclosure imposed by virtue of section 109(4)).
 - (3) Head 2 is – 35
 - (a) a disclosure made to, or authorised by, a Judicial Commissioner;
 - (b) a disclosure made to the Independent Police Complaints Commission for the purposes of facilitating the carrying out of any of its functions.
 - (4) Head 3 is – 40
 - (a) a disclosure made –
 - (i) in contemplation of, or in connection with, any legal proceedings, and
 - (ii) for the purposes of those proceedings;
 - (b) a disclosure made –

- (i) by a professional legal adviser (“L”) to L’s client or a representative of L’s client, or
 - (ii) by L’s client, or by a representative of L’s client, to L, in connection with the giving, by L to L’s client, of advice about the effect of the provisions of this Part. 5
- (5) But a disclosure within Head 3 is not an authorised disclosure if it is made with a view to furthering any criminal purpose.
- (6) Head 4 is –
 - (a) a disclosure which –
 - (i) is made by a telecommunications operator in accordance with a requirement imposed by regulations made by the Secretary of State, and 10
 - (ii) relates to the number of warrants under this Part to which the operator has given effect or has been involved in giving effect;
 - (b) a disclosure of information that does not relate to any particular warrant under this Part but relates to such warrants in general. 15

116 Offence of making unauthorised disclosure

- (1) A person commits an offence if –
 - (a) the person discloses any matter in breach of section 114(1), and
 - (b) the person knew that the disclosure was in breach of that section. 20
- (2) A person who is guilty of an offence under this section is liable –
 - (a) on summary conviction in England and Wales –
 - (i) to imprisonment for a term not exceeding 12 months (or 6 months, if the offence was committed before the commencement of section 154(1) of the Criminal Justice Act 2003), or 25
 - (ii) to a fine,
 or to both;
 - (b) on summary conviction in Scotland –
 - (i) to imprisonment for a term not exceeding 12 months, or 30
 - (ii) to a fine not exceeding the statutory maximum,
 or to both;
 - (c) on summary conviction in Northern Ireland –
 - (i) to imprisonment for a term not exceeding 6 months, or 35
 - (ii) to a fine not exceeding the statutory maximum,
 or to both;
 - (d) on conviction on indictment, to imprisonment for a term not exceeding 5 years or to a fine, or to both.
- (3) In proceedings against any person for an offence under this section in respect of any disclosure, it is a defence for the person to show that the person could not reasonably have been expected, after first becoming aware of the matter disclosed, to take steps to prevent the disclosure. 40

117 Restriction on issue of warrants to certain law enforcement officers

- (1) A law enforcement chief specified in subsection (2) may not issue a targeted equipment interference warrant under section 96 unless the law enforcement chief considers that there is a British Islands connection.
- (2) The law enforcement chiefs specified in this subsection are – 5
- (a) the Chief Constable of a police force maintained under section 2 of the Police Act 1996;
 - (b) the Commissioner, or an Assistant Commissioner, of the metropolitan police force;
 - (c) the Commissioner of Police for the City of London; 10
 - (d) the chief constable of the Police Service of Scotland;
 - (e) the Chief Constable or a Deputy Chief Constable of the Police Service of Northern Ireland;
 - (f) the Chief Constable of the British Transport Police;
 - (g) the Chief Constable of the Ministry for Defence Police; 15
 - (h) the Police Investigations and Review Commissioner.
- (3) The Director General of the National Crime Agency may not issue a targeted equipment interference warrant on the application of a member of a collaborative police force unless the Director General considers that there is a British Islands connection 20
“Collaborative police force” has the meaning given by paragraph 2 of Part 3 of Schedule 6.
- (4) For the purpose of this section, there is a British Islands connection if –
- (a) any of the conduct authorised by the warrant would take place in the British Islands (regardless of the location of the equipment that would, or may, be interfered with), 25
 - (b) any of the equipment which would, or may, be interfered with would, or may, be in the British Islands at some time while the interference is taking place, or
 - (c) a purpose of the interference is to obtain – 30
 - (i) communications sent by, or to, a person who is, or whom the law enforcement officer believes to be, for the time being in the British Islands,
 - (ii) information relating to an individual who is, or whom the law enforcement officer believes to be, for the time being in the British Islands, or 35
 - (iii) equipment data which forms part of, or is connected with, communications or information falling with sub-paragraph (i) or (ii).
- (5) Except as provided by subsections (1) to (3), a targeted equipment interference warrant may be issued under section 96 whether or not the person who has power to issue the warrant considers that there is a British Islands connection. 40

118 Part 5: interpretation

- (1) In this Part –
- “communication” includes – 45
 - (a) anything comprising speech, music, sounds, visual images or data of any description, and

- (b) signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus;
- “equipment” means equipment producing electromagnetic, acoustic or other emissions or any device capable of being used in connection with such equipment; 5
- “equipment data” has the meaning given by section 89;
- “private information” includes information relating to a person’s private or family life;
- “protected material”, in relation to a targeted examination warrant, has the meaning given by section 88(9); 10
- “senior official” means –
 - (a) in the case of a targeted equipment interference warrant which is or may be issued by the Secretary of State or a law enforcement chief, or in the case of a targeted examination warrant which is or may be issued by the Secretary of State, a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty’s Diplomatic Service; 15
 - (b) in the case of a targeted equipment interference warrant or a targeted examination warrant which is or may be issued by the Scottish Ministers, a member of the staff of the Scottish Administration who is a member of the Senior Civil Service; 20
- “targeted examination warrant” has the meaning given by section 88(9).
- (2) See also –
 - section 223 (telecommunications definitions), 25
 - section 225 (general definitions),
 - section 226 (index of defined expressions).

PART 6

BULK WARRANTS

CHAPTER 1 30

BULK INTERCEPTION WARRANTS

Bulk interception warrants

119 Bulk interception warrants

- (1) For the purposes of this Act a “bulk interception warrant” is a warrant issued under this Chapter which meets conditions A and B. 35
- (2) Condition A is that the main purpose of the warrant is one or more of the following –
 - (a) the interception of overseas-related communications (see subsection (3));
 - (b) the obtaining of secondary data from such communications (see section 120). 40
- (3) In this Chapter “overseas-related communications” means –

- (9) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve such a decision, the Secretary of State may ask the Investigatory Powers Commissioner to decide whether to approve the decision.
 - (10) A direction under subsection (3)— 5
 - (a) may not be revoked;
 - (b) may be varied but only for the purpose of altering or removing any provision included in the direction under subsection (5).
 - (11) The head of an intelligence service may, at the same time as applying for a direction under subsection (3), apply for a specific BPD warrant under section 178 (and the Secretary of State may issue such a warrant at the same time as giving the direction). 10
 - (12) In this section, “associated regulatory provision”, in relation to a power of an intelligence service to retain or examine a bulk personal dataset, means any provision which— 15
 - (a) is made by or for the purposes of this Act (other than this Part), and
 - (b) applied in relation to the retention, examination, disclosure or other use of the bulk personal dataset immediately before the giving of a direction under subsection (3).
- 193 Interpretation of Part** 20
- (1) In this Part—
 - “class BPD warrant” has the meaning given by section 175(3)(a);
 - “specific BPD warrant” has the meaning given by section 175(3)(b);
 - “senior official” means a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty’s Diplomatic Service. 25
 - (2) See also—
 - section 225 (general definitions),
 - section 226 (index of defined expressions).

PART 8 30

OVERSIGHT ARRANGEMENTS

CHAPTER 1

INVESTIGATORY POWERS COMMISSIONER AND OTHER JUDICIAL COMMISSIONERS

The Commissioners

- 194 Investigatory Powers Commissioner and other Judicial Commissioners** 35
- (1) The Prime Minister must appoint—
 - (a) the Investigatory Powers Commissioner, and
 - (b) such number of other Judicial Commissioners as the Prime Minister considers necessary for the carrying out of the functions of the Judicial Commissioners. 40

- (2) A person is not to be appointed as the Investigatory Powers Commissioner or another Judicial Commissioner unless the person holds or has held a high judicial office (within the meaning of Part 3 of the Constitutional Reform Act 2005).
- (3) Before appointing any person under subsection (1), the Prime Minister must consult—
 - (a) the Lord Chief Justice of England and Wales,
 - (b) the Lord President of the Court of Session,
 - (c) the Lord Chief Justice of Northern Ireland,
 - (d) the Scottish Ministers, and
 - (e) the First Minister and deputy First Minister in Northern Ireland.
- (4) Before appointing a Judicial Commissioner under subsection (1)(b), the Prime Minister must also consult the Investigatory Powers Commissioner.
- (5) The Prime Minister must have regard to a memorandum of understanding agreed between the Prime Minister and the Scottish Ministers when exercising functions under subsection (1) or (3)(d).
- (6) The Investigatory Powers Commissioner is a Judicial Commissioner and the Investigatory Powers Commissioner and the other Judicial Commissioners are to be known, collectively, as the Judicial Commissioners.
- (7) The Investigatory Powers Commissioner may, to such extent as the Investigatory Powers Commissioner may decide, delegate the exercise of functions of the Investigatory Powers Commissioner to any other Judicial Commissioner.
- (8) References in any enactment—
 - (a) to a Judicial Commissioner are to be read as including the Investigatory Powers Commissioner, and
 - (b) to the Investigatory Powers Commissioner are to be read, so far as necessary for the purposes of subsection (7), as references to the Investigatory Powers Commissioner or any other Judicial Commissioner.

195 Terms and conditions of appointment

- (1) Subject as follows, each Judicial Commissioner holds and vacates office in accordance with their terms and conditions of appointment.
- (2) Each Judicial Commissioner is to be appointed for a term of three years.
- (3) A person who ceases to be a Judicial Commissioner (otherwise than under subsection (5)) may be re-appointed under section 194(1).
- (4) A Judicial Commissioner may not, subject to subsection (5), be removed from office before the end of the term for which the Commissioner is appointed unless a resolution approving the removal has been passed by each House of Parliament.
- (5) A Judicial Commissioner may be removed from office by the Prime Minister if, after the appointment of the Commissioner –
 - (a) a bankruptcy order is made against the Commissioner or the Commissioner’s estate is sequestrated or the Commissioner makes a

- composition or arrangement with, or grants a trust deed for, the Commissioner’s creditors,
- (b) any of the following orders is made against the Commissioner –
 - (i) a disqualification order under the Company Directors Disqualification Act 1986 or the Company Directors Disqualification (Northern Ireland) Order 2002, 5
 - (ii) an order under section 429(2)(b) of the Insolvency Act 1986 (failure to pay under county court administration order),
 - (iii) an order under section 429(2) of the Insolvency Act 1986 (disabilities on revocation of county court administration order), 10
 - (c) the Commissioner’s disqualification undertaking is accepted under section 7 or 8 of the Company Directors Disqualification Act 1986 or under the Company Directors Disqualification (Northern Ireland) Order 2002, or 15
 - (d) the Commissioner is convicted in the United Kingdom, the Channel Islands or the Isle of Man of an offence and receives a sentence of imprisonment (whether suspended or not).

Main functions of Commissioners

- 196 Main oversight functions** 20
- (1) The Investigatory Powers Commissioner must keep under review (including by way of audit, inspection and investigation) the exercise by public authorities of statutory functions relating to –
 - (a) the interception of communications,
 - (b) the acquisition or retention of communications data, 25
 - (c) the acquisition of secondary data or related systems data under Chapter 1 of Part 2 or Chapter 1 of Part 6, or
 - (d) equipment interference.
 - (2) Such statutory functions include, in particular, functions relating to the disclosure, retention or other use of – 30
 - (a) any content of communications intercepted by an interception authorised or required by a warrant under Chapter 1 of Part 2 or Chapter 1 of Part 6,
 - (b) acquired or retained communications data,
 - (c) data acquired as mentioned in subsection (1)(c), or 35
 - (d) communications, equipment data or other information acquired by means of equipment interference.
 - (3) The Investigatory Powers Commissioner must keep under review (including by way of audit, inspection and investigation) –
 - (a) the acquisition, retention, use or disclosure of bulk personal datasets by an intelligence service, 40
 - (b) the giving and operation of notices under section 216 (national security notices),
 - (c) the exercise of functions by virtue of section 80 of the Serious Crime Act 2015 (prevention or restriction of use of communication devices by prisoners etc.), 45

PART 9

MISCELLANEOUS AND GENERAL PROVISIONS

CHAPTER 1

MISCELLANEOUS

Combined warrants and authorisations 5

212 Combination of warrants and authorisations

Schedule 8 (which makes provision for the combination of certain warrants and authorisations in a single instrument) has effect.

Compliance with Act

213 Payments towards certain compliance costs 10

- (1) *The Secretary of State must ensure that arrangements are in force for securing that telecommunications operators and postal operators receive an appropriate contribution in respect of such of their relevant costs as the Secretary of State considers appropriate.*
- (2) In subsection (1) “relevant costs” means costs incurred, or likely to be incurred, by telecommunications operators and postal operators in complying with this Act. 15
- (3) The arrangements may provide for payment of a contribution to be subject to terms and conditions determined by the Secretary of State.
- (4) Such terms and conditions may, in particular, include a condition on the operator concerned to comply with any audit that may reasonably be required to monitor the claim for costs. 20
- (5) The arrangements may provide for the Secretary of State to determine –
 - (a) the scope and extent of the arrangements, and
 - (b) the appropriate level of contribution which should be made in each case. 25
- (6) Different levels of contribution may apply for different cases or descriptions of case but the appropriate contribution must never be nil.
- (7) A retention notice under Part 4 given to a telecommunications operator or a postal operator, or a national security notice under section 216 given to a telecommunications operator, must specify the level or levels of contribution which the Secretary of State has determined should be made in respect of the costs incurred, or likely to be incurred, by the operator as a result of the notice in complying with that Part or (as the case may be) with the national security notice. 30
- (8) *For the purpose of complying with this section the Secretary of State may make, or arrange for the making of, payments out of money provided by Parliament.* 35

214 Power to develop compliance systems etc.

- (1) The Secretary of State may –

- (a) develop, provide, maintain or improve, or
- (b) enter into financial or other arrangements with any person for the development, provision, maintenance or improvement of, such apparatus, systems or other facilities or services as the Secretary of State considers appropriate for enabling or otherwise facilitating compliance by the Secretary of State, another public authority or any other person with this Act. 5
- (2) *Arrangements falling within subsection (1)(b) may, in particular, include arrangements consisting of the giving of financial assistance by the Secretary of State.*
- (3) *Such financial assistance –*
 - (a) *may, in particular, be given by way of –* 10
 - (i) *grant,*
 - (ii) *loan,*
 - (iii) *guarantee or indemnity,*
 - (iv) *investment, or*
 - (v) *incurring expenditure for the benefit of the person assisted, and* 15
 - (b) *may be given subject to terms and conditions determined by the Secretary of State.*
- (4) *Terms and conditions imposed by virtue of subsection (3)(b) may include terms and conditions as to repayment with or without interest.*

Additional powers 20

215 Amendments of the Intelligence Services Act 1994

- (1) The Intelligence Services Act 1994 is amended as follows.
- (2) In section 3 (the Government Communications Headquarters) –
 - (a) in subsection (1)(a), after “monitor” insert “, make use of”, and
 - (b) in the words following subsection (1)(b)(ii), for the words from “or to any other organisation” to the end substitute “or, in such cases as it considers appropriate, to other organisations or persons, or to the general public, in the United Kingdom or elsewhere.” 25
- (3) In section 5 (warrants: general) –
 - (a) in subsection (2), omit “, subject to subsection (3) below,” 30
 - (b) omit subsection (3),
 - (c) in subsection (3A), after “1989” insert “, or on the application of the Intelligence Service or GCHQ for the purposes of the exercise of their functions by virtue of section 1(2)(c) or 3(2)(c),”.

216 National security notices 35

- (1) The Secretary of State may give any telecommunications operator in the United Kingdom a notice (a “national security notice”) requiring the operator to take such specified steps as the Secretary of State considers necessary in the interests of national security.
- (2) The Secretary of State may give a national security notice only if the Secretary of State considers that the conduct required by the notice is proportionate to what is sought to be achieved by that conduct. 40

- (3) A national security notice may, in particular, require the operator to whom it is given—
 - (a) to carry out any conduct, including the provision of services or facilities, for the purpose of—
 - (i) facilitating anything done by an intelligence service under any enactment other than this Act, or 5
 - (ii) dealing with an emergency (within the meaning of Part 1 of the Civil Contingencies Act 2004);
 - (b) to provide services or facilities for the purpose of assisting an intelligence service to carry out its functions more securely or more effectively. 10
- (4) But a national security notice may not require the taking of any steps the main purpose of which is to do something for which a warrant or authorisation is required under this Act.
- (5) A national security notice must specify such period as appears to the Secretary of State to be reasonable as the period within which the steps specified in the notice are to be taken. 15
- (6) Sections 218 to 220 contain further provision about national security notices.

217 Maintenance of technical capability

- (1) The Secretary of State may give a relevant operator a notice (a “technical capability notice”)— 20
 - (a) imposing on the relevant operator any applicable obligations specified in the notice, and
 - (b) requiring the person to take all the steps specified in the notice for the purpose of complying with those obligations. 25
- (2) In this section—
 - “applicable obligation”, in relation to a relevant operator of a particular description, means an obligation specified by the Secretary of State in regulations as an obligation that may be imposed on relevant operators, or on relevant operators of that description; 30
 - “relevant operator” means—
 - (a) a postal operator,
 - (b) a telecommunications operator, or
 - (c) a person who is proposing to become a postal operator or a telecommunications operator. 35
- (3) Regulations under this section may specify an obligation that may be imposed on any relevant operators only if the Secretary of State considers it is reasonable to do so for the purpose of securing—
 - (a) that it is (and remains) practicable to impose requirements on those relevant operators to provide assistance in relation to relevant authorisations (see subsection (9)), and 40
 - (b) that it is (and remains) practicable for those relevant operators to comply with those requirements.
- (4) The obligations that may be specified in regulations under this section include, among other things— 45
 - (a) obligations to provide facilities or services of a specified description;

- (b) obligations relating to apparatus owned or operated by a relevant operator;
 - (c) obligations relating to the removal by a relevant operator of electronic protection applied by or on behalf of that operator to any communications or data; 5
 - (d) obligations relating to the security of any postal or telecommunications services provided by a relevant operator;
 - (e) obligations relating to the handling or disclosure of any information.
- (5) Before making any regulations under this section, the Secretary of State must consult the following persons— 10
- (a) the Technical Advisory Board,
 - (b) persons appearing to the Secretary of State to be likely to be subject to any obligations specified in the regulations,
 - (c) persons representing persons falling within paragraph (b), and
 - (d) persons with statutory functions in relation to persons falling within that paragraph. 15
- (6) The only steps that may be specified in a technical capability notice given to a person are steps which the Secretary of State considers to be necessary for securing that the person has the capability to provide any assistance which the person may be required to provide in relation to any relevant authorisation. 20
- (7) A technical capability notice must specify such period as appears to the Secretary of State to be reasonable as the period within which the steps specified in the notice are to be taken.
- (8) A technical capability notice may be given to persons outside the United Kingdom (and may require things to be done, or not to be done, outside the United Kingdom). 25
- (9) In this section “relevant authorisation” means—
- (a) any warrant issued under Part 2, 5 or 6, or
 - (b) any authorisation or notice given under Part 3.
- (10) Sections 218 to 220 contain further provision about technical capability notices. 30
- 218 Further provision about notices under section 216 or 217**
- (1) In this section “relevant notice” means—
- (a) a national security notice under section 216, or
 - (b) a technical capability notice under section 217.
- (2) Before giving a relevant notice to a person, the Secretary of State must consult that person. 35
- (3) Before giving a relevant notice, the Secretary of State must, among other matters, take into account—
- (a) the likely benefits of the notice,
 - (b) the likely number of users (if known) of any postal or telecommunications service to which the notice relates, 40
 - (c) the technical feasibility of complying with the notice,
 - (d) the likely cost of complying with the notice, and
 - (e) any other effect of the notice on the person (or description of person) to whom it relates. 45

- (4) Where the relevant notice would impose any obligations relating to the removal by a person of electronic protection applied by or on behalf of that person to any communications or data, in complying with subsection (3) the Secretary of State must in particular take into account the technical feasibility, and likely cost, of complying with those obligations. 5
- (5) A relevant notice must be in writing.
- (6) A technical capability notice may be given to a person outside the United Kingdom in any of the following ways (as well as by electronic or other means of giving a notice) –
 - (a) by delivering it to the person’s principal office within the United Kingdom or, if the person has no such office in the United Kingdom, to any place in the United Kingdom where the person carries on business or conducts activities; 10
 - (b) if the person has specified an address in the United Kingdom as one at which the person, or someone on the person’s behalf, will accept documents of the same description as a notice, by delivering it to that address. 15
- (7) The Secretary of State may by regulations make further provision about the giving of relevant notices.
- (8) A person to whom a relevant notice is given, or any person employed or engaged for the purposes of that person’s business, must not disclose the existence or contents of the notice to any other person without the permission of the Secretary of State. 20
- (9) A person to whom a relevant notice is given must comply with the notice.
- (10) The duty imposed by subsection (9) is enforceable – 25
 - (a) in relation to a person in the United Kingdom, and
 - (b) so far as relating to a technical capability notice within subsection (11), in relation to a person outside the United Kingdom,
 by civil proceedings by the Secretary of State for an injunction, or for specific performance of a statutory duty under section 45 of the Court of Session Act 1988, or for any other appropriate relief. 30
- (11) A technical capability notice is within this subsection if it relates to any of the following –
 - (a) a targeted interception warrant or mutual assistance warrant under Chapter 1 of Part 2; 35
 - (b) a bulk interception warrant;
 - (c) an authorisation or notice given under Part 3.

219 Variation and revocation of notices

- (1) In this section “relevant notice” means –
 - (a) a national security notice under section 216, or 40
 - (b) a technical capability notice under section 217.
- (2) The Secretary of State must keep each relevant notice under review.
- (3) The Secretary of State may –
 - (a) vary a relevant notice;
 - (b) revoke a relevant notice (whether wholly or in part). 45

170

- (4) The Secretary of State may vary a national security notice only if the Secretary of State considers that the conduct required by the notice as varied is proportionate to what is sought to be achieved by that conduct.
- (5) If the Secretary of State varies or revokes a relevant notice given to any person, the Secretary of State must give that person notice of the variation or revocation. 5
- (6) Subsections (2) to (4) and (7) of section 218 apply in relation to varying or revoking a relevant notice as they apply in relation to giving a relevant notice.
- (7) Subsections (5) and (6) of section 218 apply to any notice of the variation or revocation of a relevant notice as they apply to a relevant notice. 10
- (8) The fact that a relevant notice has been revoked in relation to a particular person (or description of persons) does not prevent the giving of another relevant notice of the same kind in relation to the same person (or description of persons).
- (9) Any reference in this section or section 218(8) to (11) to a notice given under section 216 or 217 includes a reference to such a notice as varied under this section. 15

220 Review by the Secretary of State

- (1) A person who is given a notice under section 216 or 217 may, within such period or circumstances as may be provided for by regulations made by the Secretary of State, refer the notice back to the Secretary of State. 20
- (2) Such a reference may be in relation to the whole of a notice or any aspect of it.
- (3) There is no requirement for a person who has referred a notice under subsection (1) to comply with the notice, so far as referred, until the Secretary of State has reviewed the notice in accordance with subsection (4). 25
- (4) The Secretary of State must review any notice so far as referred to the Secretary of State under subsection (1).
- (5) Before deciding the review, the Secretary of State must consult—
 - (a) the Technical Advisory Board, and
 - (b) the Investigatory Powers Commissioner. 30
- (6) The Board must consider the technical requirements and the financial consequences, for the person who has made the reference, of the notice so far as referred.
- (7) The Commissioner must consider whether the notice so far as referred is proportionate. 35
- (8) The Board and the Commissioner must—
 - (a) give the person concerned and the Secretary of State the opportunity to provide evidence, or make representations, to them before reaching their conclusions, and
 - (b) report their conclusions to— 40
 - (i) the person, and
 - (ii) the Secretary of State.

- (9) The Secretary of State may, after considering the conclusions of the Board and the Commissioner –
 - (a) vary or revoke the notice under section 219, or
 - (b) give a notice under this section to the person confirming its effect.
- (10) Subsections (5) to (8) of section 218 apply in relation to a notice under subsection (9)(b) above as they apply in relation to a notice under section 216 or 217. 5
- (11) Any reference in this section to a notice under section 216 or 217 includes such a notice as varied under section 219, but only so far as the variation is concerned. 10
 But it does not include a notice varied as mentioned in subsection (9)(a) above.

Wireless telegraphy

221 Amendments of the Wireless Telegraphy Act 2006

- (1) The Wireless Telegraphy Act 2006 is amended as follows.
- (2) Section 48 (interception and disclosure of messages) is amended as follows. 15
- (3) In subsection (1), for “otherwise than under the authority of a designated person” substitute “without lawful authority”.
- (4) After subsection (3) insert –
 - “(3A) A person does not commit an offence under this section consisting in any conduct if the conduct –
 - (a) constitutes an offence under section 2 of the Investigatory Powers Act 2016 (offence of unlawful interception), or
 - (b) would do so in the absence of any lawful authority (within the meaning of section 5 of that Act).”20
- (5) Omit subsection (5). 25
- (6) Omit section 49 (interception authorities).
- (7) In consequence of the repeal made by subsection (6) –
 - (a) in sections 50(5) and 119(2)(a), for “49” substitute “48”;
 - (b) in section 121(2), omit paragraph (b).

CHAPTER 2 30

GENERAL

Review of operation of Act

222 Review of operation of Act

- (1) The Secretary of State must, within the period of 6 months beginning with the end of the initial period, prepare a report on the operation of this Act. 35
- (2) In subsection (1) “the initial period” is the period of 5 years and 6 months beginning with the day on which this Act is passed.

- (3) In preparing the report under subsection (1), the Secretary of State must, in particular, take account of any report on the operation of this Act made by a Select Committee of either House of Parliament (whether acting alone or jointly).
- (4) The Secretary of State must— 5
 - (a) publish the report prepared under subsection (1), and
 - (b) lay a copy of it before Parliament.

Interpretation

223 Telecommunications definitions

- (1) The definitions in this section have effect for the purposes of this Act. 10

Communication

- (2) “Communication”, in relation to a telecommunications operator, telecommunications service or telecommunication system, includes— 15
 - (a) anything comprising speech, music, sounds, visual images or data of any description, and
 - (b) signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus.

Entity data

- (3) “Entity data” means any data which— 20
 - (a) is about— 25
 - (i) an entity,
 - (ii) an association between a telecommunications service and an entity, or
 - (iii) an association between any part of a telecommunication system and an entity,
 - (b) consists of, or includes, data which identifies or describes the entity (whether or not by reference to the entity’s location), and
 - (c) is not events data.

Events data 30

- (4) “Events data” means any data which identifies or describes an event (whether or not by reference to its location) on, in or by means of a telecommunication system where the event consists of one or more entities engaging in a specific activity at a specific time.

Communications data 35

- (5) “Communications data”, in relation to a telecommunications operator, telecommunications service or telecommunication system, means entity data or events data— 40
 - (a) which is (or is to be or is capable of being) held or obtained by, or on behalf of, a telecommunications operator and—
 - (i) is about an entity to which a telecommunications service is provided and relates to the provision of the service,

- (ii) is comprised in, included as part of, attached to or logically associated with a communication (whether by the sender or otherwise) for the purposes of a telecommunication system by means of which the communication is being or may be transmitted, or 5
 - (iii) does not fall within sub-paragraph (i) or (ii) but does relate to the use of a telecommunications service or a telecommunication system,
 - (b) which is available directly from a telecommunication system and falls within sub-paragraph (ii) of paragraph (a), or 10
 - (c) which –
 - (i) is (or is to be or is capable of being) held or obtained by, or on behalf of, a telecommunications operator,
 - (ii) is about the architecture of a telecommunication system, and
 - (iii) is not about a specific person, 15
- but does not include any content of a communication or anything which, in the absence of subsection (6)(b), would be content of a communication.

Content of a communication

- (6) “Content”, in relation to a communication and a telecommunications operator, telecommunications service or telecommunication system, means any element of the communication, or any data attached to or logically associated with the communication, which reveals anything of what might reasonably be considered to be the meaning (if any) of the communication, but – 20
 - (a) any meaning arising from the fact of the communication or from any data relating to the transmission of the communication is to be disregarded, and 25
 - (b) anything which is systems data is not content.

Other definitions

- (7) “Entity” means a person or thing.
- (8) “Public telecommunications service” means any telecommunications service which is offered or provided to the public, or a substantial section of the public, in any one or more parts of the United Kingdom. 30
- (9) “Public telecommunication system” means a telecommunication system located in the United Kingdom –
 - (a) by means of which any public telecommunications service is provided, or 35
 - (b) which consists of parts of any other telecommunication system by means of which any such service is provided.
- (10) “Telecommunications operator” means a person who –
 - (a) offers or provides a telecommunications service to persons in the United Kingdom, or 40
 - (b) controls or provides a telecommunication system which is (wholly or partly) –
 - (i) in the United Kingdom, or
 - (ii) controlled from the United Kingdom. 45

- (11) “Telecommunications service” means any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the person providing the service).
- (12) For the purposes of subsection (11), the cases in which a service is to be taken to consist in the provision of access to, and of facilities for making use of, a telecommunication system include any case where a service consists in or includes facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of such a system. 5
- (13) “Telecommunication system” means a system (including the apparatus comprised in it) that exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electromagnetic energy. 10
- (14) “Private telecommunication system” means any telecommunication system which— 15
 - (a) is not a public telecommunication system,
 - (b) is attached, directly or indirectly, to a public telecommunication system (whether or not for the purposes of the communication in question), and
 - (c) includes apparatus which is both located in the United Kingdom and used (with or without other apparatus) for making the attachment to that public telecommunication system. 20

224 Postal definitions

- (1) The definitions in this section have effect for the purposes of this Act.
Communication 25
- (2) “Communication”, in relation to a postal operator or postal service (but not in the definition of “postal service” in this section), includes anything transmitted by a postal service.
Communications data
- (3) “Communications data”, in relation to a postal operator or postal service, means— 30
 - (a) postal data comprised in, included as part of, attached to or logically associated with a communication (whether by the sender or otherwise) for the purposes of a postal service by means of which it is being or may be transmitted, 35
 - (b) information about the use made by any person of a postal service (but excluding any content of a communication (apart from information within paragraph (a)), or
 - (c) information not within paragraph (a) or (b) that is (or is to be) held or obtained by or on behalf of a person providing a postal service, is about those to whom the service is provided by that person and relates to the service so provided. 40

Postal data

- (4) “Postal data” means data which—

- (a) identifies, or purports to identify, any person, apparatus or location to or from which a communication is or may be transmitted,
 - (b) identifies or selects, or purports to identify or select, apparatus through which, or by means of which, a communication is or may be transmitted, 5
 - (c) identifies, or purports to identify, the time at which an event relating to a communication occurs, or
 - (d) identifies the data or other data as data comprised in, included as part of, attached to or logically associated with a particular communication.
- For the purposes of this definition “data”, in relation to a postal item, includes anything written on the outside of the item. 10

Other definitions

- (5) “Postal item” means—
 - (a) any letter, postcard or other such thing in writing as may be used by the sender for imparting information to the recipient, or 15
 - (b) any packet or parcel.
- (6) “Postal operator” means a person providing a postal service to persons in the United Kingdom.
- (7) “Postal service” means a service that—
 - (a) consists in the following, or in any one or more of them, namely, the collection, sorting, conveyance, distribution and delivery (whether in the United Kingdom or elsewhere) of postal items, and 20
 - (b) has as its main purpose, or one of its main purposes, to make available, or to facilitate, a means of transmission from place to place of postal items containing communications. 25
- (8) “Public postal service” means a postal service that is offered or provided to the public, or a substantial section of the public, in any one or more parts of the United Kingdom.

225 General definitions

- (1) In this Act— 30
 - “apparatus” includes any equipment, machinery or device (whether physical or logical) and any wire or cable,
 - “civil proceedings” means any proceedings in or before any court or tribunal that are not criminal proceedings,
 - “crime” means conduct which— 35
 - (a) constitutes one or more criminal offences, or
 - (b) is, or corresponds to, any conduct which, if it all took place in any one part of the United Kingdom, would constitute one or more criminal offences,
 - “criminal proceedings” includes proceedings before a court in respect of a service offence within the meaning of the Armed Forces Act 2006 (and references to criminal prosecutions are to be read accordingly), 40
 - “data” includes data which is not electronic data and any information (whether or not electronic),
 - “destroy”, in relation to electronic data, means delete the data in such a way as to make access to the data impossible (and related expressions are to be read accordingly), 45

- “enactment” means an enactment whenever passed or made; and includes –
- (a) an enactment contained in subordinate legislation within the meaning of the Interpretation Act 1978,
 - (b) an enactment contained in, or in an instrument made under, an Act of the Scottish Parliament, 5
 - (c) an enactment contained in, or in an instrument made under, a Measure or Act of the National Assembly for Wales, and
 - (d) an enactment contained in, or in an instrument made under, Northern Ireland legislation, 10
- “enhanced affirmative procedure” is to be read in accordance with section 229,
- “functions” includes powers and duties,
- “GCHQ” has the same meaning as in the Intelligence Services Act 1994,
- “head”, in relation to an intelligence service, means – 15
- (a) in relation to the Security Service, the Director-General,
 - (b) in relation to the Secret Intelligence Service, the Chief, and
 - (c) in relation to GCHQ, the Director,
- “Her Majesty’s forces” has the same meaning as in the Armed Forces Act 2006, 20
- “identifying data” has the meaning given by subsection (2),
- “intelligence service” means the Security Service, the Secret Intelligence Service or GCHQ,
- “the Investigatory Powers Commissioner” means the person appointed under section 194(1)(a) (and the expression is also to be read in accordance with section 194(8)(b)), 25
- “the Investigatory Powers Tribunal” means the tribunal established under section 65 of the Regulation of Investigatory Powers Act 2000,
- “items subject to legal privilege” –
- (a) in relation to England and Wales, has the same meaning as in the Police and Criminal Evidence Act 1984 (see section 10 of that Act), 30
 - (b) in relation to Scotland, means –
 - (i) communications between a professional legal adviser and the adviser’s client, or 35
 - (ii) communications made in connection with, or in contemplation of, legal proceedings and for the purposes of those proceedings,
 - which would, by virtue of any rule of law relating to the confidentiality of communications, be protected in legal proceedings from disclosure, and 40
 - (c) in relation to Northern Ireland, has the same meaning as in the Police and Criminal Evidence (Northern Ireland) Order 1989 (S.I. 1989/1341 (N.I. 12)) (see Article 12 of that Order),
- “Judicial Commissioner” means a person appointed under section 194(1)(a) or (b) (and the expression is therefore to be read in accordance with section 194(8)(a)), 45
- “legal proceedings” means –
- (a) civil or criminal proceedings in or before a court or tribunal, or
 - (b) proceedings before an officer in respect of a service offence within the meaning of the Armed Forces Act 2006, 50

- “modify” includes amend, repeal or revoke (and related expressions are to be read accordingly),
- “person” (other than in Parts 2 and 5) includes an organisation and any association or combination of persons,
- “person holding office under the Crown” includes any servant of the Crown and any member of Her Majesty’s forces, 5
- “primary legislation” means –
- (a) an Act of Parliament,
 - (b) an Act of the Scottish Parliament,
 - (c) a Measure or Act of the National Assembly for Wales, or 10
 - (d) Northern Ireland legislation,
- “public authority” means a public authority within the meaning of section 6 of the Human Rights Act 1998, other than a court or tribunal,
- “serious crime” means crime where –
- (a) the offence, or one of the offences, which is or would be constituted by the conduct concerned is an offence for which a person who has reached the age of 18 (or, in relation to Scotland or Northern Ireland, 21) and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of 3 years or more, or 15 20
 - (b) the conduct involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose,
- “specified”, in relation to an authorisation, warrant, notice or regulations, means specified or described in the authorisation, warrant, notice or (as the case may be) regulations (and “specify” is to be read accordingly), 25
- “subordinate legislation” means –
- (a) subordinate legislation within the meaning of the Interpretation Act 1978, or
 - (b) an instrument made under an Act of the Scottish Parliament, Northern Ireland legislation or a Measure or Act of the National Assembly for Wales, 30
- “systems data” has the meaning given by subsection (4),
- “the Technical Advisory Board” means the Board provided for by section 211, 35
- “working day” means a day other than a Saturday, a Sunday, Christmas Day, Good Friday or a bank holiday under the Banking and Financial Dealings Act 1971 in any part of the United Kingdom.
- (2) In this Act “identifying data” means –
- (a) data which may be used to identify, or assist in identifying, any person, apparatus, system or service, 40
 - (b) data which may be used to identify any event, or
 - (c) data which may be used to identify the location of any person, event or thing.
- (3) For the purposes of subsection (2), the reference to data which may be used to identify any event includes – 45
- (a) data relating to the fact of the event;
 - (b) data relating to the type, method or pattern of event;
 - (c) data relating to the time or duration of the event.

- (4) In this Act “systems data” means any data that enables or facilitates, or identifies or describes anything connected with enabling or facilitating, the functioning of any of the following –
 - (a) a postal service;
 - (b) a telecommunication system (including any apparatus forming part of the system); 5
 - (c) any telecommunications service provided by means of a telecommunication system;
 - (d) a relevant system (including any apparatus forming part of the system);
 - (e) any service provided by means of a relevant system. 10
- (5) For the purposes of subsection (4), a system is a “relevant system” if any communications or other information are held on or by means of the system.
- (6) For the purposes of this Act detecting crime or serious crime is to be taken to include –
 - (a) establishing by whom, for what purpose, by what means and generally in what circumstances any crime or (as the case may be) serious crime was committed, and 15
 - (b) the apprehension of the person by whom any crime or (as the case may be) serious crime was committed.
- (7) References in this Act to the examination of material obtained under a warrant are references to the material being read, looked at or listened to by the persons to whom it becomes available as a result of the warrant. 20

226 Index of defined expressions

In this Act, the expressions listed in the left-hand column have the meaning given by, or are to be interpreted in accordance with, the provisions listed in the right-hand column. 25

<i>Expression</i>	<i>Provision</i>	
Apparatus	Section 225(1)	
Bulk equipment interference warrant	Section 154(1)	
Bulk interception warrant	Section 119(1)	30
Civil proceedings	Section 225(1)	
Communication	Sections 223(2) and 224(2)	
Communications data	Sections 223(5) and 224(3)	
Content of a communication (in relation to a telecommunications operator, telecommunications service or telecommunication system)	Section 223(6)	35
Crime	Section 225(1)	
Criminal proceedings	Section 225(1)	
Criminal prosecution	Section 225(1)	
Data	Section 225(1)	40

Investigatory Powers Bill
Part 9 – Miscellaneous and general provisions
Chapter 2 – General

179

<i>Expression</i>	<i>Provision</i>	
Destroy (in relation to electronic data) and related expressions	Section 225(1)	
Detecting crime or serious crime	Section 225(6)	
Enactment	Section 225(1)	5
Enhanced affirmative procedure	Section 225(1)	
Entity	Section 223(7)	
Entity data	Section 223(3)	
Events data	Section 223(4)	
Examination (in relation to material obtained under a warrant)	Section 225(7)	10
Functions	Section 225(1)	
GCHQ	Section 225(1)	
Head (in relation to an intelligence service)	Section 225(1)	
Her Majesty's forces	Section 225(1)	15
Identifying data	Section 225(2) and (3)	
Intelligence service	Section 225(1)	
Interception of communication (postal service)	Sections 3(7) and 4	
Interception of communication (telecommunication system)	Sections 3(1) to (6) and 4(1)	
Interception of communication in the United Kingdom	Section 3(8)	20
Internet connection record	Section 54(6)	
Investigatory Powers Commissioner	Section 225(1)	
Investigatory Powers Tribunal	Section 225(1)	
Items subject to legal privilege	Section 225(1)	
Judicial Commissioner	Section 225(1)	25
Judicial Commissioners	Section 194(6)	
Lawful authority (in relation to interception of communication)	Section 5	
Legal proceedings	Section 225(1)	
Modify (and related expressions)	Section 225(1)	30
Person (other than in Parts 2 and 5)	Section 225(1)	
Person holding office under the Crown	Section 225(1)	
Postal data	Section 224(4)	
Postal item	Section 224(5)	
Postal item in course of transmission by postal service	Section 3(7)	35

<i>Expression</i>	<i>Provision</i>	
Postal operator	Section 224(6)	
Postal service	Section 224(7)	
Primary legislation	Section 225(1)	
Private telecommunication system	Section 223(14)	5
Public authority	Section 225(1)	
Public postal service	Section 224(8)	
Public telecommunications service	Section 223(8)	
Public telecommunication system	Section 223(9)	
Serious crime	Section 225(1)	10
Source of journalistic information	Section 68(7)	
Specified and specify (in relation to an authorisation, warrant, notice or regulations)	Section 225(1)	
Subordinate legislation	Section 225(1)	
Systems data	Section 225(4) and (5)	15
Technical Advisory Board	Section 225(1)	
Telecommunications operator	Section 223(10)	
Telecommunications service	Section 223(11) and (12)	
Telecommunication system	Section 223(13)	
Working day	Section 225(1)	20

Supplementary provision

227 Offences by bodies corporate etc.

- (1) This section applies if an offence under this Act is committed by a body corporate or a Scottish partnership.
- (2) If the offence is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of –
 - (a) a senior officer of the body corporate or Scottish partnership, or
 - (b) a person purporting to act in such a capacity,
 the senior officer or person (as well as the body corporate or partnership) is guilty of the offence and liable to be proceeded against and punished accordingly.
- (3) In this section –
 - “director”, in relation to a body corporate whose affairs are managed by its members, means a member of the body corporate,
 - “senior officer” means –

- (a) in relation to a body corporate, a director, manager, secretary or other similar officer of the body corporate, and
- (b) in relation to a Scottish partnership, a partner in the partnership.

228 Regulations 5

- (1) Any power of the Secretary of State or the Treasury to make regulations under this Act—
 - (a) is exercisable by statutory instrument,
 - (b) may be exercised so as to make different provision for different purposes or different areas, and 10
 - (c) includes power to make supplementary, incidental, consequential, transitional, transitory or saving provision.

- (2) See sections 63(3) and 64(6) for the procedure for a statutory instrument containing regulations under section 62 to which section 63 applies or (as the case may be) regulations under section 64(4) to which section 64(5) applies (enhanced affirmative procedure). 15

- (3) A statutory instrument containing regulations under —
 - (a) section 10(4) or 232(2) which amend or repeal any provision of primary legislation,
 - (b) section 39(2), 20
 - (c) section 45(4),
 - (d) section 74,
 - (e) section 80(1),
 - (f) section 205,
 - (g) section 211, 25
 - (h) section 217,
 - (i) section 220(1), or
 - (j) paragraph 33 of Schedule 8,

may not be made unless a draft of the instrument has been laid before, and approved by a resolution of, each House of Parliament. 30

- (4) A statutory instrument containing —
 - (a) regulations under section 10(4) or 232(2) to which subsection (3) does not apply,
 - (b) regulations under section 56(5), or
 - (c) regulations under paragraph 2(1)(b) of Schedule 5, 35

is (if a draft of the instrument has not been laid before, and approved by a resolution of, each House of Parliament) subject to annulment in pursuance of a resolution of either House of Parliament.

- (5) A statutory instrument containing —
 - (a) regulations under section 8(3), 40
 - (b) regulations under section 50(7)(a),
 - (c) regulations under section 62 to which section 63 does not apply,
 - (d) regulations under section 64(4) to which section 64(5) does not apply,
 - (e) regulations under section 115(6)(a), or
 - (f) regulations under section 218(7), 45

is subject to annulment in pursuance of a resolution of either House of Parliament.

- (6) A statutory instrument containing regulations under paragraph 4 of Schedule 5 is subject to annulment in pursuance of a resolution of the House of Commons. 5
- (7) See paragraphs 4(4) and 5(5) of Schedule 7 for the procedure for a statutory instrument containing regulations about the coming into force of a code of practice under that Schedule or of any revisions to such a code of practice (affirmative procedure or, in the case of the coming into force of revisions, a choice between that procedure and laying before Parliament after being made). 10
- (8) A statutory instrument containing regulations which are subject to a particular parliamentary procedure under this Act may also include regulations which are subject to a different or no parliamentary procedure under this Act (but this subsection does not apply to regulations mentioned in subsection (2), (4), (6) or (7)). 15
- (9) A statutory instrument which, by virtue of subsection (8), contains regulations which are subject to different parliamentary procedures, or one or more parliamentary procedure and no parliamentary procedure, is subject to whichever procedure is the higher procedure; and the order is as follows (the highest first) – 20
 - (a) the procedure set out in subsection (3) (the affirmative procedure),
 - (b) the procedure set out in subsection (5) above (the negative procedure),
 - (c) no procedure.
- (10) Provision is not prevented from being included in regulations made under this Act merely because the provision could have been included in other regulations made under this Act which would have been subject to a different or no parliamentary procedure. 25

229 Enhanced affirmative procedure

- (1) For the purposes of regulations under section 62 to which section 63 applies and regulations under section 64(4) to which section 64(5) applies, the enhanced affirmative procedure is as follows. 30
- (2) Subsection (3) applies if – 35
 - (a) the Secretary of State has consulted under section 63(2) or (as the case may be) 64(5) in relation to making such regulations,
 - (b) a period of at least 12 weeks, beginning with the day on which any such consultation first began, has elapsed, and
 - (c) the Secretary of State considers it appropriate to proceed with making such regulations.
- (3) The Secretary of State must lay before Parliament – 40
 - (a) draft regulations, and
 - (b) a document which explains the regulations.
- (4) The Secretary of State may make regulations in the terms of the draft regulations laid under subsection (3) if, after the end of the 40-day period, the draft regulations are approved by a resolution of each House of Parliament.
- (5) But subsections (6) to (9) apply instead of subsection (4) if – 45

- (a) either House of Parliament so resolves within the 30-day period, or
 - (b) a committee of either House charged with reporting on the draft regulations so recommends within the 30-day period and the House to which the recommendation is made does not by resolution reject the recommendation within that period. 5
- (6) The Secretary of State must have regard to –
- (a) any representations,
 - (b) any resolution of either House of Parliament, and
 - (c) any recommendations of a committee of either House of Parliament charged with reporting on the draft regulations, 10
- made during the 60-day period with regard to the draft regulations.
- (7) If after the end of the 60-day period the draft regulations are approved by a resolution of each House of Parliament, the Secretary of State may make regulations in the terms of the draft regulations.
- (8) If after the end of the 60-day period the Secretary of State wishes to proceed with the draft regulations but with material changes, the Secretary of State may lay before Parliament – 15
- (a) revised draft regulations, and
 - (b) a statement giving a summary of the changes proposed.
- (9) If the revised draft regulations are approved by a resolution of each House of Parliament, the Secretary of State may make regulations in the terms of the revised draft regulations. 20
- (10) For the purposes of this section regulations are made in the terms of draft regulations or revised draft regulations if they contain no material changes to the provisions of the draft, or revised draft, regulations. 25
- (11) References in this section to the “30-day”, “40-day” and “60-day” periods in relation to any draft regulations are to the periods of 30, 40 and 60 days beginning with the day on which the draft regulations were laid before Parliament; and, for this purpose, no account is to be taken of any time during which Parliament is dissolved or prorogued or during which either House is adjourned for more than four days. 30

230 Financial provisions

There is to be paid out of money provided by Parliament –

- (a) *any expenditure incurred by a Minister of the Crown or government department by virtue of this Act, and* 35
- (b) *any increase attributable to this Act in the sums payable by virtue of any other Act out of money so provided.*

231 Transitional, transitory or saving provision

- (1) Schedule 9 (which contains transitional, transitory and saving provision including a general saving for lawful conduct) has effect. 40
- (2) The Secretary of State may by regulations make such transitional, transitory or saving provision as the Secretary of State considers appropriate in connection with the coming into force of any provision of this Act.

232 Minor and consequential provision

- (1) Schedule 10 (which contains minor and consequential provision) has effect.
- (2) The Secretary of State may by regulations make such provision as the Secretary of State considers appropriate in consequence of this Act.
- (3) The power to make regulations under subsection (2) may, in particular, be exercised by modifying any provision made by or under an enactment. 5

Final provision

233 Commencement, extent and short title

- (1) Subject to subsections (2) and (3), this Act comes into force on such day as the Secretary of State may by regulations appoint; and different days may be appointed for different purposes. 10
- (2) Sections 222 to 230, 231(2), 232(2) and (3) and this section come into force on the day on which this Act is passed.
- (3) Sections 194 and 195 come into force at the end of the period of two months beginning with the day on which this Act is passed. 15
- (4) Subject to subsections (5) and (6), this Act extends to England and Wales, Scotland and Northern Ireland.
- (5) An amendment, repeal or revocation of an enactment has the same extent as the enactment amended, repealed or revoked.
- (6) Her Majesty may by Order in Council provide for any of the provisions of this Act to extend, with or without modifications, to any of the British overseas territories. 20
- (7) This Act may be cited as the Investigatory Powers Act 2016.

Exhibit P

3/2/2016

Written evidence - Apple Inc and Apple Distribution International

Apple Inc. and Apple Distribution International—written evidence (IPB0093)

1. The world today faces security threats from criminals and terrorists who threaten our shared commitment to a peaceful and productive future. Apple has a long history of cooperating with the UK government on a wide range of important issues, and in that tradition, thanks the Committee for the opportunity to share our views on this topic.
2. Apple is deeply committed to protecting public safety and shares the Government's determination to combat terrorism and other violent crimes. Strong encryption is vital to protecting innocent people from malicious actors. While the Government has said it does not intend to weaken encryption, its representatives have made clear if, "the Secretary of State and a judicial commissioner think there is necessity and proportionality in order to be able to provide that information, those companies should be required to provide that information in the clear."
3. The fact is to comply with the Government's proposal, the personal data of millions of law-abiding citizens would be less secure.

Summary

4. Hundreds of millions of people depend on Apple's products and services. Our customers trust Apple and their Apple devices with some of their most personal information — their financial data, health data, family photos, videos and messages.
5. Two things have changed in a short period of time: 1) the amount of sensitive information innocent individuals put on their devices; and 2) the sophistication and determination of malicious cyber-attackers. Governments, businesses, and individuals have all been victims, and we've all been surprised by the successful implementation of exploits the experts viewed as still merely theoretical.
6. Increasingly sophisticated hacking schemes and cyber-attacks have become the new normal as individuals live more of their lives on their devices and online. Without strong defense, these attacks have the potential to impose chaos, and threaten our way of life, economic stability and infrastructure.
7. We owe it to our customers to protect their personal data to the best of our ability. Increasingly stronger — not weaker — encryption is the best way to protect against these threats.
8. The bill threatens to hurt law-abiding citizens in its effort to combat the few bad actors who have a variety of ways to carry out their attacks. The creation of backdoors and intercept capabilities would weaken the protections built into Apple products and endanger all our customers. A key left under the doormat would not just be there for the good guys. The bad guys would find it too.
9. Encryption today is as ubiquitous as computing itself and we are all the better for it. There are hundreds of products that use encryption to protect user data, many of them open-source and beyond the regulation of any one government. By mandating weakened encryption in Apple products, this bill will put law-abiding citizens at risk, not the criminals, hackers and terrorists who will continue having access to encryption.
10. Some would portray this as an all-or-nothing proposition for law enforcement. Nothing

3/2/2016

Written evidence - Apple Inc and Apple Distribution International

could be further from the truth. Law enforcement today has access to more data — data which they can use to prevent terrorist attacks, solve crimes and help bring perpetrators to justice — than ever before in the history of our world.

11. If the UK Government forces these capabilities, there's no assurance they will not be imposed in other places where protections are absent.

12. On the pages that follow, our submission will also take exception to the fact the bill would attempt to force non-UK companies to take actions that violate the laws of their home countries. This would immobilize substantial portions of the tech sector and spark serious international conflicts. It would also likely be the catalyst for other countries to enact similar laws, paralyzing multinational corporations under the weight of what could be dozens or hundreds of contradictory country-specific laws.

13. Finally, the bill would also force companies to expend considerable resources hacking their own systems at the Government's direction. This mandate would require Apple to alter the design of our systems and could endanger the privacy and security of users in the UK and elsewhere.

14. We are committed to doing everything in our power to create a safer and more secure world for our customers. But it is our belief this world cannot come by sacrificing personal security.

Encryption

15. Every day, over a trillion transactions occur safely over the Internet as a result of encrypted communications. These range from online banking and credit card transactions to the exchange of healthcare records, ideas that will change the world for the better, and communications between loved ones. Governments like the United States fund sophisticated encryption technology including some of the best end-to-end encryption apps. Encryption, in short, *protects people*.

16. Protecting our customers and earning their trust is fundamental to our business model. At Apple, we've been providing customers easy ways to protect their data with strong encryption in our products and services for well over 10 years. In 2003, we launched FileVault to protect data on a user's Mac. In 2010, with iOS 4, we began to encrypt data on iOS devices to keys derived from a user's passcode. We launched FaceTime in 2010 and iMessage in 2011, both with end-to-end encryption. As users increasingly entrust Apple and their devices with sensitive information, we will continue to deploy strong encryption methods because we firmly believe they're in our customers' best interests, and ultimately in the best interests of humanity. Our job is to constantly stay 10 steps ahead of the bad guys.

17. Some have asserted that, given the expertise of technology companies, they should be able to construct a system that keeps the data of nearly all users secure but still allows the data of very few users to be read covertly when a proper warrant is served. But the Government does not know in advance which individuals will become targets of investigation, so the encryption system necessarily would need to be compromised for everyone.

18. The best minds in the world cannot rewrite the laws of mathematics. Any process that weakens the mathematical models that protect user data will by extension weaken the protection. And recent history is littered with cases of attackers successfully implementing exploits that nearly all experts either remained unaware of or viewed as merely theoretical. Every day that companies hold the ability to decrypt their customers' data is more time criminals have to gain that ability. All the while, hacking technology grows more sophisticated. What might have been adequate security

3/2/2016

Written evidence - Apple Inc and Apple Distribution International

for customers two years ago no longer is and that's why we've strengthened our encryption protections.

19. Strong encryption does not eliminate Apple's ability to give law enforcement metadata or other categories of data, as outlined in our Law Enforcement Guidelines. The information Apple and other companies provide helps catch criminals and save lives. It is for this reason that UK law enforcement still requests this data from us routinely. Information about our assistance can be found at <http://www.apple.com/privacy/government-information-requests/>

20. We believe it would be wrong to weaken security for hundreds of millions of law-abiding customers so that it will also be weaker for the very few who pose a threat. In this rapidly-evolving cyber-threat environment, companies should remain free to implement strong encryption to protect customers.

Extraterritoriality

21. Apple has been established in Europe for more than 35 years. With the exception of certain limited retail and human resources data, Apple is not established in the UK.

22. Under European data protection law, Apple Distribution International established in Cork, Ireland and iTunes S.à.r.l. established in Luxembourg have data controller responsibility for Apple and iTunes user personal data of users located in the EEA and Switzerland.

23. We take this responsibility very seriously and face sanction from data protection authorities and/or user litigation if we fail to meet those requirements. Additionally, user content is stored in the United States, and US law controls access to that data by law enforcement. Failure on the part of any relevant US entity to follow those requirements gives rise to criminal and civil liability. Most relevant, Title III of the US Omnibus Crime Control and Safe Streets Act would subject Apple to criminal sanctions for any unauthorized interception of content in transit.

24. As defined in relevant EU Telecommunications Law, Apple is not an electronic communications service provider. The Investigatory Powers Bill seeks to extend definitions in this area to an extent beyond that provided for in relevant EU law.

25. The draft bill makes explicit its reach beyond UK borders to, in effect, any service provider with a connection to UK consumers. In short, we believe this will lead to major issues for businesses and could ultimately put UK users at greater risk.

26. The first problem with asserting such extraterritorial powers is that there will remain a proportion of service providers which will never assist British law enforcement regardless of threatened sanction because they are underground or in jurisdictions unfriendly to British interests. It is to these providers that dangerous people will gravitate.

27. Even leaving that aside, the implications for companies such as Apple who do assist law enforcement will be profound. As well as complying with local law in the countries where we are established for the provision of our services, we will have to attempt to overlay compliance with UK law. On their face, those laws would not be in harmony. Further, we know that the IP bill process is being watched closely by other countries. If the UK asserts jurisdiction over Irish or American businesses, other states will too.

28. Those businesses affected will have to cope with a set of overlapping foreign and

3/2/2016

Written evidence - Apple Inc and Apple Distribution International

domestic laws. When these laws inevitably conflict, the businesses will be left having to arbitrate between them, knowing that in doing so they might risk sanctions. That is an unreasonable position to be placed in.

29. The Government has partly addressed this by providing a defense for businesses who cannot comply with a warrant because of local laws (although not in all parts of the bill - see below). However, once a third jurisdiction is overlaid (home country, UK and one other), the situation soon becomes very difficult for businesses to negotiate.

30. This will not just be an issue for companies like Apple: any British business with customers overseas might be faced with having to comply with a warrant from a foreign jurisdiction which poses it ethical problems, or impinges on the privacy of British consumers.

31. Clearly this situation could arise regardless of whatever legislation is passed in the UK. But Parliament will be leading the way with this bill and needs to carefully consider the precedent it sets.

Equipment Interference

32. We believe the UK is the first national Government to attempt to provide a legislative basis for equipment interference. Consumer trust in the public and private sectors can benefit from a more concrete understanding of the framework in which these activities can take place. However, it could at the same time be undermined by a blurring of the boundaries of responsibilities, and the bill as it stands seems to threaten to extend responsibility for hacking from Government to the private sector.

33. It would place businesses like Apple - whose relationship with customers is in part built on a sense of trust about how data will be handled - in a very difficult position. For the consumer in, say, Germany, this might represent hacking of their data by an Irish business on behalf of the UK state under a bulk warrant - activity which the provider is not even allowed to confirm or deny. Maintaining trust in such circumstances will be extremely difficult.

34. For these reasons, we believe there is a need for much greater clarity as to how the powers in the bill will be applied, not least because, once again, the extension of the powers to overseas providers will set a precedent which, if followed by other countries, could endanger the privacy and security of users in the UK and elsewhere.

Specific Comments on Clauses

Clauses 189, 190 and 191

35. These clauses govern the Secretary of State's ability to require businesses to establish a technical capability to comply with warrants.

36. Paragraphs (1) to (5) of Clause 189 would authorize the Secretary of State to make regulations imposing specified obligations on an operator. Paragraph (4) states that those obligations could include ones "relating to the removal of electronic protection applied by a relevant operator to any communications or data" in other words, the removal of encryption.

37. As set out above, we believe there are significant risks to applying this power to encryption and to extending this power to overseas providers. We therefore do not believe the clause should be retained in its current form and certainly should not extend outside the UK.

3/2/2016

Written evidence - Apple Inc and Apple Distribution International

38. However, this power could have a very profound effect on any business to whom the clauses apply, and the details are worth examining.
39. First, the oversight seems less rigorous than other parts of the bill. There is no judicial authorization of the requirements placed on businesses. There is no protection for businesses who cannot comply because of local laws.
40. Second, the system does not allow for a full weighing of the costs of compliance. While the clauses require some assessment of compliance cost, it is not clear how this would be calculated. Even if a consensus could be reached on the number of working hours and computing power needed to comply, a proper consideration would need to include the opportunity cost as other projects were put on hold, the knock-on effects for other services and the change in the customer relationship.
41. Third, because (as we explain above) any reduction in encryption in the UK will be exploited by regimes and bad actors not subject to the same privacy and civil liberties protections as UK law enforcement, the implications of a Notice under these clauses would go way beyond either the UK or the affected business. The bill at present does not require any consideration of this.
42. Fourth, there is no explicit obligation for the requirements on a business to be proportionate. Our reading of the bill is that although the Secretary of State might be required to take into account the benefits, costs and technical feasibility of the notice, and consult the Technical Advisory Board and (in the case of review) the Investigatory Powers Commissioner, it is at best implicit that she must only impose requirements that are proportionate. If there is a review, the bill requires that the Investigatory Powers Commissioner must consider whether the notice is proportionate, but the Secretary of State could still reject this advice.
43. The overall effect is a wide ranging power for the Secretary of State to demand a business remove encryption based on an insufficiently robust process and without regard to the full effects, leaving the business with no effective means of appeal.
44. Suggested amendments:
- The steps required of a business by a Notice should not include removal of electronic protection.
- These powers should not extend to overseas businesses; a conflict of laws exemption should be added.
- A notice under s189 should require judicial authorization.
- There should be clear and concise definitions for the following terms: "removal of electronic protection", "technical feasibility" and "reasonably practicable". These are key terms that should not be left in the first instance for argument in court. Parliament should define and agree what their intent is.
- The criteria by which the assessment is made by the Secretary of State should be made much more explicit.
- The Technical Advisory Board advice should be made available to the affected business, and in the case of a review under clause 191, the Interception Commissioner's advice as well.
- Before imposing any requirement under s189, the Secretary of State should consider whether the time spent in complying, cost (including opportunity cost), knock-on effects and change in customer relationships are reasonable and proportionate to the expected benefits.

3/2/2016

Written evidence - Apple Inc and Apple Distribution International

The Secretary of State should also be obliged to consider the impact of a notice on human rights, in the UK and globally.

The Secretary of State should be required only to apply notices that are proportionate as advised by the Commissioner.

Clause 188

45. Paragraph (1) of Clause 188 would authorize the Secretary of State to give any telecommunications operator in the UK a national security notice directing the operator to take such steps as the Secretary of State considers necessary in the interests of national security. 188(4) precludes the powers under this clause being used as a shortcut if powers exist elsewhere in the bill.

46. While we take the strong view that this bill should not be used to demand the removal of encryption, we would not want to see that clarified only for a catch-all Clause 188 to allow the Secretary of State to demand it unilaterally.

47. Suggested amendment:

The Clause should be amended to clarify that it cannot be used to require businesses to remove electronic protection from their products or services.

Clause 31

48. This clause places a duty on an operator to comply with a warrant. Again, in line with our argument above, we continue to believe the duty should not be applied to overseas businesses, but have some more general comments on the clause.

49. Clause 31 would require a relevant operator to take all reasonably practicable steps for giving effect to a warrant. Although this is not explicit in the draft bill, our understanding of the government's intention is that this would require us to remove end to end encryption if that was necessary to give effect to the warrant and considered proportionate. The Home Office indicated exactly this in the evidence to your committee we quoted above.

50. In other words, the bill as it stands means that whether or not the Secretary of State has served a business with a Clause 189 order requiring it to remove electronic protection, a fresh warrant could be served on a business requiring them to provide data in the clear, backed up by the threat of imprisonment. This seems to represent a short cut for the Secretary of State to insist on removal of encryption - but of course compliance with a warrant in the timescale required by a criminal investigation is likely to be impossible.

51. Suggested amendments:

This Clause should not apply to overseas providers.

The Clause should be amended to make clear that 'reasonably practicable steps' cannot include removal of electronic protection unless dealt with separately under a Notice under Clause 189, subject to the amendments to that Clause we suggest above.

The definition of 'reasonably practicable steps' should be clarified as we set out above to distinguish it from 'technical feasibility.'

Clauses 81 and 135

3/2/2016

Written evidence - Apple Inc and Apple Distribution International

52. These clauses deal with targeted and bulk equipment interference warrants.
53. We are concerned about the way in which the bill could make private companies implicated in the hacking of their customers.
54. Clause 81(2) provides that a warrant can be served on a person to require them to assist in hacking.
55. Is the intention that persons receiving a warrant would knowingly let the security services break into their equipment or services or allow them to use that equipment to break into equipment used by a third party? Or does the envisaged power go even further and require persons in receipt of a warrant to actively assist in the interference of their own equipment and services?
56. These questions become even more pressing when applied to bulk equipment interference warrants. It is extremely difficult to imagine circumstances in which this could be justified, so we believe the bill must spell out in more detail the types of activities required of communications providers and the circumstances in which they are expected to carry them out. Additionally and in line with earlier comments, these clauses should not have extra-territorial effect.
57. Suggested amendments:
- The powers in this part of the bill need to be fully understood as to their intent. The bill should set out in much more detail what the requirement on a person served with a warrant will be.
- The clauses should not apply to overseas providers who would be put in an impossible conflict of laws position.

21 December 2015

Exhibit Q

Facebook Inc., Google Inc., Microsoft Corp., Twitter Inc., Yahoo Inc.—written evidence (IPB0116)

INTRODUCTION

1. National security is an important concern for Governments. Governments have a responsibility to protect people and their privacy. We believe a legal framework can protect both. Our companies want to help establish a framework for lawful requests for data that, consistent with principles of necessity and proportionality, protects the rights of the individual and supports legitimate investigations.
2. As members of the Reform Government Surveillance (RGS) coalition (www.reformgovernmentsurveillance.com), we believe the best way for countries to promote the security and privacy interests of their citizens, while also respecting the sovereignty of other nations, is to ensure that surveillance is targeted, lawful, proportionate, necessary, jurisdictionally bounded, and transparent. These principles reflect the perspective of global companies that offer borderless technologies to billions of people around the globe.
3. The actions the UK Government takes here could have far reaching implications – for our customers, for your own citizens, and for the future of the global technology industry. While we recognize the UK Government has made efforts to develop a clear, comprehensive and modern legal framework, we would offer several important considerations that shape our view of the Bill:
 - User trust is essential to our ability to continue to innovate and offer our customers products and services, which empower them to achieve more in their personal and professional lives.
 - Governments' surveillance authorities, even when transparent and enshrined in law, can undermine users' trust in the security of our products and services.
 - Key elements of whatever legislation is passed by the UK are likely to be replicated by other countries, including with respect to UK citizens' data.
 - Unilateral imposition of obligations on overseas providers will conflict with legal obligations such providers are subject to in other countries.
 - An increasingly chaotic international legal system will leave companies in the impossible position of deciding whose laws to violate and could fuel data localization efforts.
4. We appreciate the opportunity to consult on the Bill. To that end, we advance a number of issues that we believe are important to serve UK citizens and the citizens of other nations, while ensuring that citizens' human rights and privacy rights are protected. This includes ensuring the Bill satisfies ECJ scrutiny and also builds greater legal certainty and consistency for the proposed measures.

PRIMARY CONCERNS

1. **Extraterritorial Jurisdiction (ETJ)**
 - a) **Conflict of laws:** As noted earlier, we anticipate that other countries will emulate what the UK does here. Unilateral assertions of extraterritorial jurisdiction will create conflicting legal obligations for overseas providers who are subject to legal obligations elsewhere. The UK Government understood this in 2009, when the Home Office Consultation 'Protecting the Public in a Changing Communications Environment' stated that RIPA did not apply to overseas providers. Conflicts of laws create an increasingly chaotic legal environment for providers, restricting the free flow of information and leaving private companies to decide whose laws to violate. These decisions should be made by Governments, grounded in fundamental rights of privacy, freedom of expression, and other human rights.

If the UK legislation retains authority to reach extraterritorially, the Bill should consistently and explicitly state that no company is required to comply with any notice/warrant, which in doing so would contravene its legal obligations in other jurisdictions. Enforcement obligations should also take this into account. Notwithstanding our position, currently there is confusion: the context section of the Bill overview document states, "Enforcement of obligations against overseas CSPs will be limited to interception and targeted CD acquisition powers". This is not what the Bill itself says.

- b) **International framework:** We agree with the recommendation of Sir Nigel Sheinwald and others that an international framework should be developed to establish a common set of rules to resolve these conflicts across jurisdictions. These rules should facilitate more efficient requests in cases that provide adequate protections for user privacy. There are indications in the legislation that the UK Government has identified an approach that could work. Though interception is generally prohibited, for example, the Bill permits interception in the UK when it is done "in response to a request made in accordance with a relevant international agreement." If the UK Government's authority should have unlimited application overseas, it is unclear why the UK Government believes other countries' authorities should only extend into the UK pursuant to an international agreement. Instead, a better approach would be to condition the extraterritorial application of UK law to situations where it is done pursuant to an international agreement that permits it, and furthermore resolves conflicting obligations in the other country.
- c) **Service of warrants on overseas providers:** The Bill permits warrants to be served on companies outside the UK in a number of ways, including serving it on principal offices within the UK. Despite ETJ language, this presents a risk to UK employees of our companies. We have collective experience around the world of personnel who have nothing to do with the data sought being arrested or intimidated in an attempt to force a overseas corporation to disclose user information. We do not believe that the UK wants to legitimize this lawless and heavy-handed practice.

2. Technical impositions:

- a) **Clarity on encryption:** The companies believe that encryption is a fundamental security tool, important to the security of the digital economy as well as crucial to ensuring the safety of web users worldwide. We reject any proposals that would require companies to deliberately weaken the security of their products via backdoors, forced decryption, or any other means. We therefore have concerns that the Bill includes "*obligations relating to the removal of electronic protection applied by a relevant operator to any communication or data*" and that these are explicitly intended to apply extraterritorially with limited protections for overseas providers. We appreciate the statements in the Bill and by the Home Secretary that the Bill is not intended to weaken the use of encryption, and suggest that the Bill expressly state that nothing in the Bill should be construed to require a company to weaken or defeat its security measures.
- b) **No business should be compelled to generate and retain data that it does not ordinarily generate in the course of its business.** Some language under the retention part of the Bill suggests that a company could be required to generate data – and perhaps even reconfigure their networks or services to generate data – for the purposes of retention.

3. Judicial authorization:

- a) **Judicial review standard:** As recommended by David Anderson QC, Governments should not be able to compel the production of private communications content absent authorization from an independent and impartial judicial official. While we believe the Bill's 'double lock' represents an important step in the right direction, there remains room for improvement. The "judicial review" standard should be clarified to ensure that the judge reviews the actual merits of the matter, and not just the process by which decisions and actions were taken by the authorizing secretary. To

truly serve as a second lock, this function must not just assess the rationality or reasonableness of the ministerial decision, but ensure that investigatory warrants under the Bill will withstand the full scrutiny of a court.

- b) **Applicability:** we believe that judicial authorization should be applied to a broader set of authorities and also be extended to national security notices, maintenance of technical capability orders, and modifications to equipment interference warrants which have been issued to the Chief of Defence Intelligence and intelligence services.

4. Bulk collection

- a) **Explicit language:** As set forth in the Reform Government Surveillance principles, surveillance laws should not permit bulk collection of information. The principles require that the Government specifically identify the individuals or accounts to be targeted and should expressly prohibit bulk surveillance. The word "bulk" can be ambiguous. We understand from David Anderson QC's report that, in the UK, bulk warrants allow a specific communications channel external to the UK to be specified due to the link with a specific national security or serious crime threat. It is then filtered and searched for identifiers. In terms of setting international precedent, we therefore suggest that the Bill be more explicit in the language it uses, highlighting that any collection should be pursuant to a specific identifier.
- b) **Minimization provisions:** We also believe that the general safeguards sections should explicitly include 'minimization' provisions, ensuring that only the necessary and proportionate amount of data is obtained, analyzed and retained. All other data should be destroyed.

5. Transparency and Clarity

- a) **Elimination of Vague and Confusing Language:** As David Anderson QC highlighted in '*A Question of Trust*', legislation on surveillance powers should be written in such a way that the intelligent reader can understand the surveillance powers possessed by the Government, and how, where and by whom they are used. Legislation or practice that is wide-reaching and vague harms the ability of the users and companies to understand government surveillance. It also impacts on the ability of formal and informal oversight mechanisms, including NGOs, to carry out their function effectively. There are many aspects of the Bill which we believe remain opaque: judicial authorization; the extent of the obligations on companies outside of the UK; the confusing messages about the extent to which there is an obligation to produce material that can be read versus the Government's statement about the Bill not prohibiting encryption; and the obligations on technical capability. We outline additional suggestions in the document. We urge the Joint Committee and the Home Office to do all that it can to ensure that the whole Bill is written clearly and unambiguously.
- b) **User notification:** As a general rule, users should be informed when the Government seeks access to account data. It is important both in terms of transparency, as well as affording users the right to protect their own legal rights. Our users range from individual consumers to large media organizations to large public sector entities. Even where the Government establishes a need to obtain certain information, it does not necessarily deprive users of other rights they may have, and knowledge of the request is essential to their ability to advance those rights. While it may be appropriate to withhold or delay notice in exceptional cases, in those cases the burden should be on the Government to demonstrate that there is an overriding need to protect public safety or preserve the integrity of a criminal investigation.
- c) **Warrant recipient:** We welcome the Bill's clarification that warrants must be both "necessary and proportionate." However, once there is a determination that a warrant is necessary, the question should then be to whom the warrant should be directed. It is our view that the same standard – "necessary" – should be applied when evaluating this question. In many cases, the Government can (and often does) obtain the information directly from the users themselves. When that is not

possible, the Government should seek the information from the most proximate source with access to the data. An obvious example of this involves enterprise cloud customers. Even as private sector and public sector entities transition to the cloud, they remain in complete control of their own data. Before they moved data off of their own servers and onto the servers of large cloud providers, Governments would go to them for their data or the data of their employees. There is no reason Governments cannot continue to do the same after these organizations transition their data to the cloud. This is an area where the UK can lead the rest of the world, promoting cloud adoption, protecting law enforcement's investigative needs, and resolving jurisdictional challenges without acting extraterritorially.

- d) **Overseas provider standing:** Overseas providers should have a legal right to seek legal advice and raise complaints with the Commissioner without either committing a disclosure offence or accepting jurisdiction. There should be the possibility for judicial commissioners to request amicus briefs from affected providers.
- e) **Clarity on urgent provisions, e.g. approval of warrants issued in urgent cases.** The term "urgent" is not defined in the Bill. Clarity on this term - which other countries may seek to emulate and even abuse - is important.

6. Computer Network Exploitation:

- a) **Risk to user trust:** The ultimate test we apply to each of the authorities in this Bill is whether they will promote and maintain the trust users place in our technology. Even where these authorities do not apply to overseas providers like our companies, we are concerned that some of the authorities contained in the Bill, as currently drafted, represent a step in the wrong direction. The clearest example is the authority to engage in computer network exploitation, or equipment interference. To the extent this could involve the introduction of risks or vulnerabilities into products or services, it would be a very dangerous precedent to set, and we would urge your Government to reconsider.
- b) **Network integrity and cyber security requirements:** There are no statutory provisions relating to the importance of network integrity and cyber security, nor a requirement for agencies to inform companies of vulnerabilities that may be exploited by other actors. We urge the Government to make clear that actions taken under authorization do not introduce new risks or vulnerabilities for users or businesses, and that the goal of eliminating vulnerabilities is one shared by the UK Government. Without this, it would be impossible to see how these provisions could meet the proportionality test.

We are happy to follow up in writing with any queries you have on this written evidence, and undertake to answer, via email, within 24 hours including during the holiday period. We are also happy to provide specific drafting comments, should you wish these.

Facebook Inc.

Google Inc.

Microsoft Corp.

Twitter Inc.

Yahoo Inc.

21 December 2015

Exhibit R

Connect with us

CNET › Security › BlackBerry to leave Pakistan after refusing to ditch user privacy

BlackBerry to leave Pakistan after refusing to ditch user privacy

The Canadian company has taken a stand against demands for "backdoor" access to its services, including encrypted email and messages.

by Katie Collins @katiecollins / 1 December 2015 4:25 am AEDT

Search CNET

Reviews

News

Video

How To

Games

AU Edition

BlackBerry will shut down operations in Pakistan at year's end because demands from the country's Telecommunications Authority would result in a massive invasion of user privacy, the company said Monday.



BlackBerry says Pakistan is demanding complete access to customer information.

Andrew Hoyle/CNET

BlackBerry refuses to agree to the Pakistani government's order to monitor BlackBerry Enterprise Services (BES), including encrypted emails and BBM messages sent and received in the country. It is therefore withdrawing on December 30, Chief Operating Officer Marty Beard said in a [blog post](#) Monday. The Canadian company said it enforces a blanket ban on allowing so-called "backdoor" access to customer information anywhere in the world.

"Pakistan's demand was not a question of public safety; we are more than happy to assist law enforcement agencies in investigations of criminal activity," Beard said. "Rather, Pakistan was essentially demanding unfettered access to all of our BES customers' information."



Governments, accustomed to tapping phone lines and opening mail in decades past, want access to people's digital data to help stop crime and security threats. However, especially in the wake of revelations from former NSA contractor Edward Snowden about massive surveillance by the US and UK, tech companies have been wrestling with government data requests that they believe can go too far.

BlackBerry has long emphasized security in its sales pitch to government, military and business customers. On learning that the Pakistani government would require "wholesale" access to BlackBerry Enterprise Services, the company decided its customers' communications would be compromised to the extent that it has no choice but to leave Pakistan altogether.

BlackBerry is setting a precedent for how it will react to being told it must comply or leave, but it is far from the only company facing serious questions. The debate over encrypted communications is raging in many countries, including big markets like the US and UK that are tougher to ignore. If governments come down hard against encryption in the name of national security, tech giants like Google, Apple and Facebook will need to decide on the importance of customer privacy in countries a lot closer to home than Pakistan.

Tags: Security, BlackBerry

DISCUSS: BLACKBERRY TO LEAVE PAKISTAN AFTER REFUSING...

10 Comments

[Log In](#)

Show Comments

Featured Video

Paid Content

Google leans into its AI peek at Android N

By Brian Tong / 2 March 2016

The Surface Pro 4 Will Fuel Your Day.

Paid Content promoted by Microsoft

Mistakes millions of Britons make with their pensions
Hargreaves Lansdown

This Watch Brand Is Disrupting A \$60 Billion Industry

Exhibit S

Search

Missing Plug-in

News Views Life

Outlook 2016

Editor's Choice | Business | National | Archipelago | Jakarta | World | Sports

Government asks RIM to open access to wiretap Blackberry users

The Jakarta Post, Jakarta | Business | Thu, September 15 2011, 8:11 PM



Tifatul Sembiring

The government has urged Research in Motion (RIM), the developer of Blackberry smart phones, to open its special access to wiretap those people suspected of corruption or money laundering, and others, who are under criminal investigation.

"We will ask it to open access to people, who are allegedly involved in crimes. If RIM agrees, we will sign an agreement," Information and Communications Minister Tifatul Sembiring said, as quoted by Antara news agency on Thursday.

He added that the company had already fulfilled five out of six demands by the Indonesian government. "It has opened branches in Indonesia; offers after servicing; blocks negative content; recruits Indonesian workers; and cooperates with local content developers so as to use local software and components," said Tifatul.

The only demand that has not yet been fulfilled is for the company to open a data center in Indonesia. According to Tifatul, the company has yet to give an explanation regarding its delay, adding that RIM could be punished if it refused to open the center.

To date, there has been no legal basis for wiretapping Blackberry users, unlike other operators. With other operators, they could open

access for wiretapping if their customers have allegedly been involved in a crime. "RIM has yet to open access to wiretap Blackberry users even though the technology to allow us to do so is already available," said Tifatul.

Institutions that are given the authority to wiretap are the police, the Attorney General's Office, the Corruption Eradication Commission and the National Narcotics Agency.

Like 6

Indonesian PMA Companies

Foreign Company
Establishment, Visas, Work
Permits, Taxation

Read also:

- Research In Motion shares climb
- RIM offers free voice calls over Wi-Fi with BBM
- RIM to launch new BlackBerry software Jan. 30
- Nokia loss widens to \$1.27 billion in Q3
- Govt urges RIM to build data server in Indonesia

Post Your Say

Selected comments will be published in the Readers' Forum page of our print newspaper.

0 comments

Sign in

+ Follow Share Post comment as...

Newest | Oldest | Top Comments

Powered by Livefyre



the Jakarta Post Digital

News

Travel

News

Editor's Choice
Business
National
Archipelago
Jakarta
World

Views

Opinion
Reader's Forum
Your Voice

Life

Digital Life
Sci-tech
Environment
Body & Soul
Art & Design
Culture

Services

Contact Us
Media Kit

Exhibit T



EDITION: U.S.

SIGN IN | REGISTER

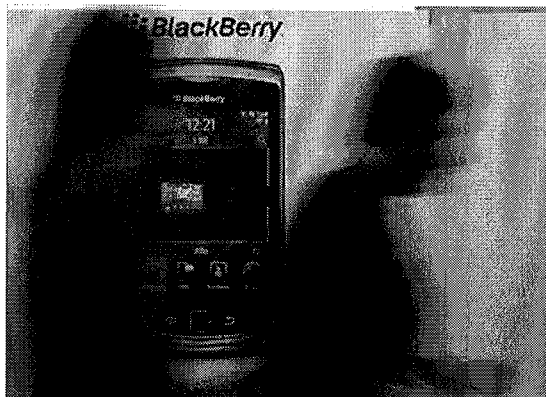
Search Reuters

[HOME](#) [BUSINESS](#) [MARKETS](#) [WORLD](#) [POLITICS](#) [TECH](#) [OPINION](#) [BREAKINGVIEWS](#) [MONEY](#) [LIFE](#) [PICTURES](#) [VIDEO](#)


Technology | Mon Apr 25, 2011 7:16am EDT

Related: TECH

BlackBerry firm seeks security "balance" in Russia



Visitors pass an advertising banner showing a BlackBerry mobile at the CeBIT computer fair in Hanover March 2, 2011. REUTERS/TOBIAS SCHWARZ

BlackBerry maker Research In Motion said Russia could help development of new technologies by finding a balance between state security and innovation.

Co-chief executive Jim Balsillie said on Monday the Canadian company had "ambitious plans" in Russia and offered President Dmitry Medvedev -- an avid user of Apple's iPad -- a new BlackBerry tablet at a meeting on developing [new technology](#).

RIM, whose BlackBerry products are used by executives and politicians including U.S. President Barack Obama, has faced demands from countries such as India and Saudi Arabia to give authorities access to its encrypted communications services.

Speaking to reporters before the Medvedev meeting, Balsillie said: "A very important (question) for Russia is how do they balance the need for letting innovative things happen, but managing state security.

Many countries grapple with this around the world," he said, adding a balance was needed that "allows innovation to happen, but still state security to be looked after".

India this year demanded full access to BlackBerry services as part of efforts to fight militancy and security threats over the internet and through telephone communications.

RIM said in January it has given India the means to access its Messenger service but reiterated no changes could be made to allow the monitoring of secure corporate emails.

RIM encrypts email messages as they travel between a BlackBerry device and a [computer](#) known as BlackBerry Enterprise Server. The company has said it does not have a master key to decode these emails and only the sponsoring business or organization has the technical capability to grant access to encrypted enterprise email.

BLACKBERRY IN RUSSIA

Russia's two biggest carriers began offering BlackBerry services in late 2007, after years of negotiations between RIM and the Federal Security Service (FSB) that did not involve handing over encryption codes.

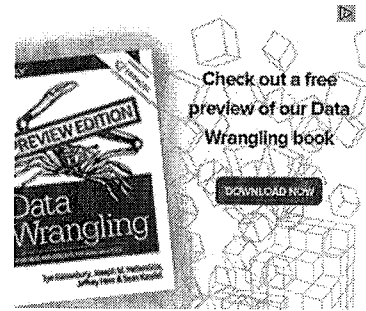
The FSB domestic spy service called earlier this month for access to encrypted communication providers like Gmail, Hotmail and Skype, saying uncontrolled use of such services could threaten national security.

Russia's communications minister, Igor Shchygolev, told Reuters ahead of Medvedev's meeting the government wanted international companies like RIM to be present on the Russian market, offering "the most up-to-date technologies".

"If there are some network security demands, and they exist globally, we need to seek compromise to provide security and at the same time not to set up barriers for companies," he said.

Balsillie said Russia was still a relatively small market for RIM meaning it had "extremely ambitious plans to sell Blackberry in Russia, invest in R&D, (and) also to invest in start-ups".

(Writing by Maria Kiselyova and Guy Faulconbridge; Editing by Dan Lalor)



PHOTOS OF THE DAY



Our top photos from the last 24 hours. [Slideshow »](#)

Super Tuesday

Pictures of the month: February

More from Reuters

- **Wife of 'American Sniper' making waves in Texas**
Republican politics
| 26 Feb
- **Wall Street's big short: President Donald J. Trump**
| 1 Mar
- **Trump vows to 'open up' libel laws if elected** | 26 Feb
- **FAA proposes fix for Boeing 787 Dreamliner** | 23 Feb
- **How the Republican elite turned a blind eye to the rise and rise of Donald Trump**
| 2 Mar
- **Exclusive: Boeing plans layoffs for airplane engineers**
| 27 Feb
- **Spy agencies say Clinton emails closely matched top secret documents: sources** | 24 Feb
- **North Korea satellite tumbling in orbit again: U.S. sources**
| 18 Feb
- **19 retired U.S. generals, admirals back Clinton's stance on Guantanamo**
| 25 Feb
- **One area where the Pentagon is playing catchup with Russia and China** | 23 Feb

Sponsored Financial Content

- **Major pensions changes: Are you ready?** *TD Direct Investing*
- **Eastern tigers roar again?** *JP Morgan*
- **Analysed: The corporate tax responsibility dilemma** *Alliance Trust*
- **Demand for sovereign bonds persists even as shares rally** *News.Markets*
- **Market review- Bank of Japan - below zero** *Aberdeen*



Now available for iPhone



Ever thought you could win the presidency?
[Download Now »](#)

TRENDING ON REUTERS

- U.N. Imposes harsh new sanctions on North Korea over its nuclear program** **1**
- Supreme Court divided in high-stakes Texas abortion case** **2**
- Mozambique plane debris believed to be from Boeing 777: Malaysia minister** **3**
- How the Republican elite turned a blind eye to the rise and rise of Donald Trump** **4**
- Bin Laden called for Americans to rise up over climate change** **5**

Exhibit U



WIRED.CO.UK

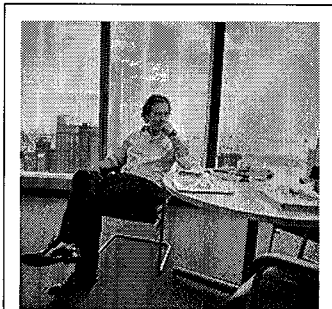
6 issues for £9 + FREE iPad & iPhone editionsSubscribe

Startups, incumbents and the future of fintech Visa Europe Collab DISCOVER MORE

BlackBerry gives Indian government ability to intercept messages

BUSINESS (/BUSINESS) / 11 JULY 13 /
by KADHIM SHUBBER (/SEARCH/AUTHOR/KADHIM+SHUBBER)

f t p in g+ ✉ 59 shares
0 comments



Am I a good father?



After years of wrangling, BlackBerry (formerly known as RIM) has finally agreed to give the Indian government the ability to intercept data sent over BlackBerry devices.

According to leaked Indian government documents seen by the *Times of India* (<http://timesofindia.indiatimes.com/tech/tech-news/telecom/Government-BlackBerry-dispute-ends/articleshow/20998679.cms>), "the lawful interception system for BlackBerry Services is ready for use".

Once implemented, the system will allow the Indian government to track emails and email attachments in real time; to see when BBM messages have been delivered and read; and to intercept web browsing data, according to the report.

Crucially, the Indian government appear to have dropped previous demands to have access to BlackBerry's Enterprise servers, which carries BlackBerry's corporate email services. Instead, BlackBerry will have to notify the authorities about which companies are using the Enterprise service.



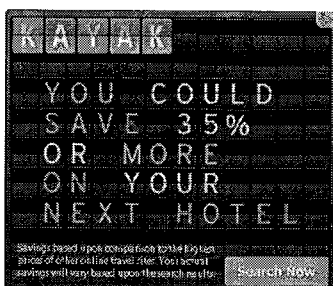
Flickr.com/Hello Turkey Toe

The soon-to-be-signed agreement will potentially end years of disagreements between BlackBerry and the Indian government, which at one point threatened to shutdown (http://www.guardian.co.uk/technology/2010/aug/13/blackberry-india-security-demands-rim) BlackBerry email and messenger in India.

Since the 2008 Mumbai killings, the Indian government has pressured BlackBerry to give it access to users' data -- BlackBerry devices were reported to have been used by the terrorists in the attacks (http://www.wired.com/dangerroom/2008/12/the-gadgets-of/).

Similar pressure has been applied on the company across the world, including the UK (http://www.wired.co.uk/news/archive/2011-08/09/why-are-we-blaming-bbm-for-riots) and Saudi Arabia (http://www.wired.co.uk/news/archive/2010-08/02/gulf-states-ban-blackberry), which recently banned Viber (http://www.wired.co.uk/news/archive/2013-06/05/viber-banned-in-saudi-arabia) after the company failed to give the Saudi government access to its users' messages.


According to the *Times of India* report, nine of the ten telecoms providers that carry BlackBerry's data will be implementing the intercept technology, which was reportedly demonstrated in Mumbai on 12 June on the Vodafone network.



BlackBerry issued the following statement: "BlackBerry has delivered a solution that enables India's wireless carriers to address their lawful access requirements for our consumer messaging services, which include BlackBerry Messenger (BBM) and BlackBerry Internet Service (BIS) email. The lawful access capability now available to BlackBerry's carrier partners meets the standard required by the Government of India for all consumer messaging services offered in the Indian marketplace. We also wish to underscore, once again, that this enablement of lawful access does not extend to BlackBerry Enterprise Server".



READ NEXT

 </news/archive/2016-03/02/wired-awake-2-mar>
WIRED AWAKE
WIRED Awake
10 must-read articles for 2 March
(/news/archiv
03/02/wired-awake-2-mar

LATEST ON WIRED.CO.UK

Exhibit V

Connect with us

Search CNET

Reviews

News

Video

How To

Games

UK Edition

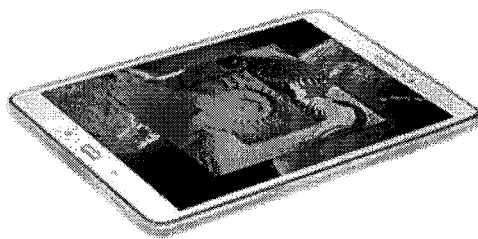
CNET > Security > RIM averts BlackBerry ban in UAE

RIM averts BlackBerry ban in UAE

Regulators in the United Arab Emirates say BlackBerry services now comply with the nation's requirements, adding that RIM cooperated in offering a reasonable fix.

by Lance Whitney @lancewhit / 8 October 2010 3:11 pm BST

SAMSUNG
Galaxy Tab A



WHERE WILL THE GALAXY TAB A TAKE YOU?

Research In Motion and the United Arab Emirates have reached an agreement to call off a BlackBerry ban that was scheduled to start Monday.

Today's press release (Google Translate version) from the Telecommunications Regulatory Authority (TRA), which regulates telecommunications for the UAE, confirmed that all BlackBerry services will continue as usual and not be suspended on October 11.



The agency said that BlackBerry services are now compatible with the UAE's regulatory framework and added that RIM had cooperated in offering a compatible solution. Beyond that, the agency offered no details as far as specific actions or measures that RIM may have taken to avert the ban.

In a response to news of the agreement with the UAE, a RIM spokesperson e-mailed CNET the following statement dated today:

"RIM cannot discuss the details of confidential regulatory matters that occur in specific countries, but RIM confirms that it continues to approach lawful access matters internationally within the framework of core principles that were publicly communicated by RIM on August 12."



A UAE BlackBerry ban would have affected around 500,000 customers in the region and hit both local residents and foreign visitors.

In early August, the UAE announced that it would shut down e-mail, instant messaging, and Web browsing for BlackBerry devices on the October 11 deadline due to RIM's failure to meet the emirates' regulatory requirements. The UAE had been putting pressure on the BlackBerry maker to open up the security on its networks so that local officials could monitor and access customer data for what they see as national security reasons.

RIM had run into similar problems with India and Saudi Arabia, both of which were also demanding access to the corporate data flowing over the company's networks. On its end, the company had insisted from the start that the information on its networks is encrypted and that it does not hold the encryption keys, therefore it can't comply with regulations to make that data available.

With international pressure mounting, RIM fought back at first. At one point, the company's co-CEO Michael Lazaridis said in a Wall Street Journal interview that if these countries can't deal with the Internet, then they should shut it off. More recently, the company's other CEO, Jim Balsillie, suggested that governments that need to monitor BlackBerry corporate data should ask the corporations themselves for access since they're the ones that hold the keys.

But faced with potential bans from multiple countries, RIM was forced to compromise. In August, the company was able to strike agreements with both India and Saudi Arabia to avert their announced bans. The accords reached in those two cases reportedly involved setting up local BlackBerry servers in those countries through which the governments will be able to access their data directly.

Tags: Security, Tech Industry, Mobile, Encryption, BlackBerry

DISCUSS: RIM AVERTS BLACKBERRY BAN IN UAE

No Comments

[Log In](#)

[Show Comments](#)

Featured Video

Paid Content

Google leans into its next peek at Android N

By Brian Tong / 2 March 2016

Purchase the Surface Pro 4 & get coffee to fuel your day.

Paid Content promoted by Microsoft

Exhibit W



EDITION: UK

SIGN IN | REGISTER

Search Reuters

HOME BUSINESS MARKETS WORLD UK TECH MONEY OPINION BREAKINGVIEWS SPORT LIFE PICTURES VIDEO



Technology | Wed Aug 11, 2010 6:27am BST

Related: BUSINESS

RIM to share some BlackBerry codes with Saudis - source

Missing Plug-in

Research In Motion RIM.TO has agreed to hand over user codes that would let Saudi authorities monitor its BlackBerry Messenger, as it seeks to stop the kingdom from silencing the service, a source close to the talks said on Tuesday.

The source said RIM would share with Saudi Arabia the unique pin number and code for each BlackBerry registered there. That will allow authorities to read encrypted text sent via Messenger, an instant messaging service that's distinct from email sent on the BlackBerry.

The arrangement would effectively give Saudi Arabia access to RIM's main server for Messenger, but only for communications to and from Saudi users, the source said..

The Canadian company declined to comment, referring media to its earlier statement in which it said it "cooperates with all governments with a consistent standard."

"I would imagine other countries are going to want to be treated in a similar way, whatever that way happens to be," said Todd Coupland at CIBC World Markets in Toronto, referring to a Saudi code sharing deal for Messenger.

Saudi Arabia, like United Arab Emirates, Kuwait, India and some other countries, has sought access to encrypted BlackBerry communications, citing social and national security concerns.

BlackBerry Messenger has proven popular with young singles in Saudi Arabia, an Islamic society that restricts contact between unrelated men and women. The country is the biggest BlackBerry market in the Gulf with 700,000 users.

Social and political activists also say BlackBerry's encrypted texting has brought more open dialogue, including criticism of governments and policies.

PHOTOS



Editor's choice

Our top photos from the last 24 hours.



TRENDING ON REUTERS

- Brexit could shrink UK's financial services industry - BlackRock **1**
- Bank of England digital cash? Watch out for the banks: Broadbent **2**
- EU cities will pounce on London business in event of Brexit - minister **3**
- Exclusive: China to lay off five to six million workers, earmarks at least \$23 billion | VIDEO **4**
- Huge quake strikes off Indonesia but tsunami warnings cancelled **5**

This use of the BlackBerry contrasts with the situation in Western countries, where the device is specially popular among business and government professionals that value its security. Email is encrypted and decrypted by BlackBerry Enterprise Servers, which RIM says are only controlled by the sponsoring business or organisation.

RIM, unlike rivals Nokia NOK1V.HE and Apple (AAPL.O), operates its own network through secure servers located in Canada and other countries such as Britain.

One analyst said RIM might give ground on servers for Messenger, but the company was unlikely to budge on the security of email sent through these Enterprise servers.

PROGRESS REPORTED

The Saudi telecom regulator said earlier it was making progress in its talks with RIM, and that the Messenger service was still up and running. It did not say what, if any, arrangement had been made with RIM.

"In light of the positive developments in completing part of the regulatory requirements from the service providers, the regulatory authority has decided to allow the continuation of the BlackBerry Messenger services," the regulator said.

Saudi Arabia had earlier said it would stop all messaging from Friday unless the two sides found a way for authorities to tap into the BlackBerry messages. It later extended that deadline to Monday.

The source said RIM initially agreed to set up a server at each of the three Saudi service providers.

But that proved impractical, so the company changed course and offered the Interior Ministry and intelligence services the codes to all Saudi BlackBerry users, said the source, who was not authorized to speak about the talks and asked not to be named.

A spokesman for the regulator, the Communications and Information Telecommunications Commission, was not available for immediate comment on the source's remarks.

QUICK RETURN TO NORMAL

RIM has declined specific comments on any talks since governments, mostly in the Middle East, have stepped up pressure to gain access to the secure BlackBerry network.

But the company's co-chief executive, Michael Lazaridis, told the Wall Street Journal last week that RIM would have to comply with a court order to intercept communications.

"I would give them the encrypted stream," he said. "It would have to be like a wiretap."


A code-sharing arrangement with Saudi Arabia would let the interior ministry monitor Messenger activity, the source said.

"It seems to be contrary to what RIM has always maintained," said Paradigm Capital analyst Barry Richards.

Abdulhamid al-Amri, a member of the Saudi Economic Association, said "things will go back to normal" once the two sides resolve the issue. He said a Saudi agreement would likely lead to early deals with other governments.

"I believe that the firm will be as responsive to the rest of the countries because it is in its interest not to play favourites between countries as that would affect its own interests," he said.

RIM still faces a more sweeping ban in the neighbouring UAE, where authorities have

Sponsored Financial Content 

Major pensions changes expected in March 2016 *TD Direct Investing*

Eastern tigers roar again? *JP Morgan*

A straightforward investment tip most investors ignore *Stanley Gibbons*

China is a boom not a doom *Baillie Gifford & Co*

Brexit Referendum: Polls and Possibilities *Henderson*

RECOMMENDED VIDEO

[Breakingviews: The Buffett Rules](#)

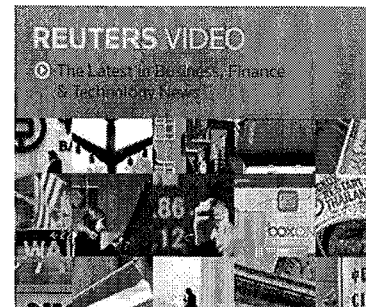
[China's 'Trojan horse' train into Hong Kong](#)

IN OR OUT?



Britain's Brexit Vote

Follow all the latest developments as Britain counts down to the June 23 referendum on EU membership. [Full Coverage »](#)



threatened to ban Messenger, emailing and web browsing on the device from October.

Saudi Telecom Co 7010.SE, the country's No.1 telecom operator, and its smaller rivals Mobily 7020.SE and Zain Saudi Arabia 7030.SE were not available for comment.

(Additional reporting by Alastair Sharp and Nicole Mordant; Writing by Jason Neely and Frank McGurty; Editing by Greg Mahlich and Janet Guttzman)



The new BlackBerry Torch 9800 smartphone is introduced at a news conference in New York August 3, 2010. REUTERS/SHANNON STAPLETON

More from Reuters

- Britain's campaign to leave EU takes 4 percent point lead - ORB poll | 26 Feb
- Analysis - EU's real brake isn't Britain but Franco-German impasse | 21 Feb
- 'Brexit' would damage UK, could sink the EU, billionaire Richard Branson says | 19 Feb
- EU's Tower of Babel may fall while leaders distracted | 29 Feb
- HSBC effectively scraps pay rise for managers at UK retail bank - source | 17 Feb
- Deeply eurosceptic Britons may still vote to stay in EU - survey | 23 Feb
- Putin says EU-Russia ties will return to normal 'sooner or later' | 17 Feb
- Kurds' advance in Syria divides U.S. and Turkey as Russia bombs | 17 Feb
- HSBC executives rue missed chance in HQ choice | 18 Feb

Sponsored Financial Content (?)

- Major pensions changes: Are you ready? *TD Direct Investing*
- Lloyds Share Offer: why demand is huge? *Galvan*
- Tax-free income *J.P. Morgan*
- Which 5 Stocks should you be buying? *Central Markets*
- Day Trading - Free 6 page guide *Guardian Stockbrokers*

Exhibit X

Advance Edited Version

Distr.: General
22 May 2015

Original: English

Human Rights Council

Twenty-ninth session

Agenda item 3

**Promotion and protection of all human rights, civil,
political, economic, social and cultural rights,
including the right to development**

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*

Summary

In the present report, submitted in accordance with Human Rights Council resolution 25/2, the Special Rapporteur addresses the use of encryption and anonymity in digital communications. Drawing from research on international and national norms and jurisprudence, and the input of States and civil society, the report concludes that encryption and anonymity enable individuals to exercise their rights to freedom of opinion and expression in the digital age and, as such, deserve strong protection.

* Late submission.

Contents

	<i>Paragraphs</i>	<i>Page</i>
I. Introduction	1–5	3
II. Secure and private communication in the digital age.....	6–13	4
A. Contemporary encryption and anonymity	6–10	4
B. Uses of the technologies	11–13	5
III. Encryption, anonymity and the rights to freedom of opinion and expression and privacy	14–28	6
A. Privacy as a gateway for freedom of opinion and expression	16–18	7
B. Right to hold opinions without interference	19–21	8
C. Right to freedom of expression.....	22–26	9
D. Roles of corporations	27–28	10
IV. Evaluating restrictions on encryption and anonymity.....	29–55	11
A. Legal framework.....	29–35	11
B. State practice: examples and concerns.....	36–55	12
V. Conclusions and recommendations	56–63	19
A. States	57–60	19
B. International organizations, private sector and civil society.....	61–63	20

I. Introduction

1. Contemporary digital technologies offer Governments, corporations, criminals and pranksters unprecedented capacity to interfere with the rights to freedom of opinion and expression. Online censorship, mass and targeted surveillance and data collection, digital attacks on civil society and repression resulting from online expression force individuals around the world to seek security to hold opinions without interference and seek, receive and impart information and ideas of all kinds. Many seek to protect their security through encryption, the scrambling of data so only intended recipients may access it, which may be applied to data in transit (e.g., e-mail, messaging, Internet telephony) and at rest (e.g., hard drives, cloud services). Others seek additional protection in anonymity, using sophisticated technologies to disguise their identity and digital footprint. Encryption and anonymity, today's leading vehicles for online security, provide individuals with a means to protect their privacy, empowering them to browse, read, develop and share opinions and information without interference and enabling journalists, civil society organizations, members of ethnic or religious groups, those persecuted because of their sexual orientation or gender identity, activists, scholars, artists and others to exercise the rights to freedom of opinion and expression.

2. Yet, just as the telephone may be used both to report a crime to the police and to conspire to commit one, so too may the Internet be abused to interfere with the rights of others, national security or public order. Law enforcement and intelligence services often assert that anonymous or encrypted communications make it difficult to investigate financial crimes, illicit drugs, child pornography and terrorism. Individuals express legitimate concerns about how bullies and criminals use new technologies to facilitate harassment. Some States restrict or prohibit encryption and anonymity on these and other grounds, while others are proposing or implementing means for law enforcement to circumvent these protections and access individual communications.

3. In the light of these challenges, the present report examines two linked questions. First, do the rights to privacy and freedom of opinion and expression protect secure online communication, specifically by encryption or anonymity? And, second, assuming an affirmative answer, to what extent may Governments, in accordance with human rights law, impose restrictions on encryption and anonymity? The present report seeks to answer these questions, review examples of State practice and propose recommendations. It does not purport to address every technical or legal question raised by digital technologies, but it identifies important ones for future reporting.

4. In preparing the report, the Special Rapporteur circulated a questionnaire to States, seeking relevant information on their domestic laws, regulations, policies and practices. As of 1 April 2015, 16 States had responded to this request.¹ The Special Rapporteur also issued a call for submissions from non-governmental stakeholders and convened a meeting of experts in Geneva in March 2015. The responses from Governments and the over 30 submissions by civil society organizations and individuals, which are available from the mandate holder's web page, contributed significantly to the preparation of the report.

5. A full review of the Special Rapporteur's activities since the beginning of his term in August 2014 may be found on the mandate holder's web page. This report, the current

¹ Responses were received from Austria, Bulgaria, Cuba, Germany, Greece, Guatemala, Ireland, Kazakhstan, Lebanon, Qatar, Republic of Moldova, Norway, Slovakia, Sweden, Turkey and the United States of America.

mandate holder's first, aims at furthering the work on the challenges to freedom of expression in the digital age.

II. Secure and private communication in the digital age

A. Contemporary encryption and anonymity

6. Modern approaches to private and secure communication draw on ideas that have been with humankind for millennia. The rise of electronic data storage, the Internet and mass data collection and retention made clear that sophisticated means would be needed to protect individual, corporate and government data. As e-mail, instant-messaging, Voice-over-Internet Protocols, videoconferencing and social media moved from niche services to predominant and easily monitored modes of communication, individuals developed a need for security online, so that they could seek, receive and impart information without the risk of repercussions, disclosure, surveillance or other improper use of their opinions and expression.

7. Encryption — a mathematical “process of converting messages, information, or data into a form unreadable by anyone except the intended recipient”² — protects the confidentiality and integrity of content against third-party access or manipulation. Strong encryption, once the sole province of militaries and intelligence services, is now publicly accessible and often freely available to secure e-mail, voice communication, images, hard drives and website browsers. With “public key encryption”, the dominant form of end-to-end security for data in transit, the sender uses the recipient's public key to encrypt the message and its attachments, and the recipient uses her or his own private key to decrypt them. Encryption may also be used to create digital signatures to ensure that a document and its sender are authentic, to authenticate and verify the identity of a server and to protect the integrity of communications between clients against tampering or manipulation of traffic by third parties (e.g., “man-in-the-middle” attacks). Since the encryption of data in transit does not ensure against attacks on unencrypted data when it is sitting at rest at either endpoint (nor protect the security of one's private key), one may also encrypt data at rest stored on laptops, hard drives, servers, tablets, mobile phones and other devices. Online practices may also be moving away from the system described here and towards “forward secrecy” or “off-the-record” technology in which keys are held ephemerally, particularly for uses such as instant messaging.

8. Some call for efforts to weaken or compromise encryption standards such that only Governments may enjoy access to encrypted communications. However, compromised encryption cannot be kept secret from those with the skill to find and exploit the weak points, whether State or non-State, legitimate or criminal. It is a seemingly universal position among technologists that there is no special access that can be made available only to government authorities, even ones that, in principle, have the public interest in mind. In the contemporary technological environment, intentionally compromising encryption, even for arguably legitimate purposes, weakens everyone's security online.

9. Notably, encryption protects the content of communications but not identifying factors such as the Internet Protocol (IP) address, known as metadata. Third parties may gather significant information concerning an individual's identity through metadata analysis if the user does not employ anonymity tools. Anonymity is the condition of avoiding identification. A common human desire to protect one's identity from the crowd,

² See SANS Institute, “History of encryption” (2001).

anonymity may liberate a user to explore and impart ideas and opinions more than she would using her actual identity. Individuals online may adopt pseudonyms (or, for instance, fake e-mail or social media accounts) to hide their identities, image, voice, location and so forth, but the privacy afforded through such pseudonyms is superficial and easily disturbed by Governments or others with the necessary expertise; in the absence of combinations of encryption and anonymizing tools, the digital traces that users leave behind render their identities easily discoverable. Users seeking to ensure full anonymity or mask their identity (such as hiding the original IP address) against State or criminal intrusion may use tools such as virtual private networks (VPNs), proxy services, anonymizing networks and software, and peer-to-peer networks.³ One well-known anonymity tool, the Tor network, deploys more than 6,000 decentralized computer servers around the world to receive and relay data multiple times so as to hide identifying information about the end points, creating strong anonymity for its users.

10. A key feature of the digital age is that technology changes incessantly to sate user demands. Although the present report refers to contemporary technologies that facilitate encryption and anonymity, its analysis and conclusions apply generally to the concepts behind the current technologies and should be applicable as new technologies replace the old.

B. Uses of the technologies

11. The Internet has profound value for freedom of opinion and expression, as it magnifies the voice and multiplies the information within reach of everyone who has access to it. Within a brief period, it has become the central global public forum. As such, an open and secure Internet should be counted among the leading prerequisites for the enjoyment of the freedom of expression today. But it is constantly under threat, a space — not unlike the physical world — in which criminal enterprise, targeted repression and mass data collection also exist. It is thus critical that individuals find ways to secure themselves online, that Governments provide such safety in law and policy and that corporate actors design, develop and market secure-by-default products and services. None of these imperatives is new. Early in the digital age, Governments recognized the essential role played by encryption in securing the global economy, using or encouraging its use to secure Government-issued identity numbers, credit card and banking information, business proprietary documents and investigations into online crime itself.⁴

12. Encryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief. For instance, they enable private communications and can shield an opinion from outside scrutiny, particularly important in hostile political, social, religious and legal environments. Where States impose unlawful censorship through filtering and other technologies, the use of encryption and anonymity may empower individuals to circumvent barriers and access information and ideas without the intrusion of authorities. Journalists, researchers, lawyers and civil society rely on encryption and anonymity to shield themselves (and their sources, clients and partners) from surveillance and harassment. The ability to search the web, develop ideas and communicate securely may be the only way in which many can explore basic aspects of identity, such as one's gender, religion, ethnicity, national origin or sexuality. Artists rely on encryption and anonymity to

³ Proxy services send data through an intermediary, or "proxy server", that sends that data on behalf of the user, effectively masking the user's IP address with its own to the end recipient. Peer-to-peer networks partition and store data among interconnected servers and then encrypt that stored data so that no centralized server has access to identifying information. See, for example, Freenet.

⁴ See OECD, *Guidelines for Cryptography Policy* (1997)..

safeguard and protect their right to expression, especially in situations where it is not only the State creating limitations but also society that does not tolerate unconventional opinions or expression.

13. The “dark” side of encryption and anonymity is a reflection of the fact that wrongdoing offline takes place online as well. Law enforcement and counter-terrorism officials express concern that terrorists and ordinary criminals use encryption and anonymity to hide their activities, making it difficult for Governments to prevent and conduct investigations into terrorism, the illegal drug trade, organized crime and child pornography, among other government objectives. Harassment and cyberbullying may rely on anonymity as a cowardly mask for discrimination, particularly against members of vulnerable groups. At the same time, however, law enforcement often uses the same tools to ensure their own operational security in undercover operations, while members of vulnerable groups may use the tools to ensure their privacy in the face of harassment. Moreover, Governments have at their disposal a broad set of alternative tools, such as wiretapping, geo-location and tracking, data-mining, traditional physical surveillance and many others, which strengthen contemporary law enforcement and counter-terrorism.⁵

III. Encryption, anonymity and the rights to freedom of opinion and expression and privacy

14. The human rights legal framework for encryption and anonymity requires, first, evaluating the scope of the rights at issue and their application to encryption and anonymity; and, second, assessing whether, and if so to what extent, restrictions may lawfully be placed on the use of technologies that promote and protect the rights to privacy and freedom of opinion and expression.

15. The rights to privacy⁶ and freedom of opinion and expression⁷ have been codified in universal and regional human rights instruments, interpreted by treaty bodies and regional courts, and evaluated by special procedures of the Human Rights Council and during universal periodic review. The universal standards for privacy, opinion and expression are found in the International Covenant on Civil and Political Rights, to which 168 States are party. Even for those remaining States that are not bound by it, the Covenant presents at the very least a standard for achievement and often reflects a customary legal norm; those that have signed but not ratified the Covenant are bound to respect its object and purpose under article 18 of the Vienna Convention on the Law of Treaties. National legal systems also protect privacy, opinion and expression, sometimes with constitutional or basic law or interpretations thereof. Several global civil society projects have also provided compelling demonstrations of the law that should apply in the context of the digital age, such as the International Principles on the Application of Human Rights to Communications

⁵ See Center for Democracy and Technology, “‘Going Dark’ versus a ‘Golden Age for Surveillance’” (2011).

⁶ Article 12 of the Universal Declaration of Human Rights, article 17 of the International Covenant on Civil and Political Rights, article 16 of the Convention on the Rights of the Child, article 22 of the Convention on the Rights of Persons with Disabilities, article 14 of the Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, article 8 of the European Convention on Human Rights and article 11 of the American Convention on Human Rights protect the right to privacy.

⁷ Article 19 of the Universal Declaration and the International Covenant on Civil and Political Rights, article 9 of the African Charter on Human and Peoples’ Rights, article 13 of the American Convention on Human Rights and article 10 of the European Convention on Human Rights protect freedom of expression.

Surveillance and the Global Principles on National Security and the Right to Information. Although specific standards may vary from right to right, or instrument to instrument, a common thread in the law is that, because the rights to privacy and to freedom of expression are so foundational to human dignity and democratic governance, limitations must be narrowly drawn, established by law and applied strictly and only in exceptional circumstances. In a digital age, protecting such rights demands exceptional vigilance.

A. Privacy as a gateway for freedom of opinion and expression

16. Encryption and anonymity provide individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks. The previous mandate holder noted that the rights to “privacy and freedom of expression are interlinked” and found that encryption and anonymity are protected because of the critical role they can play in securing those rights (A/HRC/23/40 and Corr.1). Echoing article 12 of the Universal Declaration of Human Rights, article 17 of the International Covenant on Civil and Political Rights specifically protects the individual against “arbitrary or unlawful interference with his or her privacy, family, home or correspondence” and “unlawful attacks on his or her honour and reputation”, and provides that “everyone has the right to the protection of the law against such interference or attacks”. The General Assembly, the United Nations High Commissioner for Human Rights and special procedure mandate holders have recognized that privacy is a gateway to the enjoyment of other rights, particularly the freedom of opinion and expression (see General Assembly resolution 68/167, A/HRC/13/37 and Human Rights Council resolution 20/8).

17. Encryption and anonymity are especially useful for the development and sharing of opinions, which often occur through online correspondence such as e-mail, text messaging, and other online interactions. Encryption provides security so that individuals are able “to verify that their communications are received only by their intended recipients, without interference or alteration, and that the communications they receive are equally free from intrusion” (see A/HRC/23/40 and Corr.1, para. 23). Given the power of metadata analysis to specify “an individual’s behaviour, social relationships, private preferences and identity” (see A/HRC/27/37, para. 19), anonymity may play a critical role in securing correspondence. Besides correspondence, international and regional mechanisms have interpreted privacy to involve a range of other circumstances as well.⁸

18. Individuals and civil society are subjected to interference and attack by State and non-State actors, against which encryption and anonymity may provide protection. In article 17 (2) of the International Covenant on Civil and Political Rights, States are obliged to protect privacy against unlawful and arbitrary interference and attacks. Under such an affirmative obligation, States should ensure the existence of domestic legislation that prohibits unlawful and arbitrary interference and attacks on privacy, whether committed by government or non-governmental actors. Such protection must include the right to a remedy for a violation.⁹ In order for the right to a remedy to be meaningful, individuals must be given notice of any compromise of their privacy through, for instance, weakened encryption or compelled disclosure of user data.

⁸ Human Rights Committee, general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation. See also European Court of Human Rights, factsheets on data protection (www.echr.coe.int/Documents/FS_Data_ENG.pdf) and right to protection of one’s image (www.echr.coe.int/Documents/FS_Own_image_ENG.pdf).

⁹ See Human Rights Committee general comment No. 16 and general comment No. 31 on the nature of the general legal obligation imposed on States parties to the Covenant; and CCPR/C/106/D/1803/2008.

B. Right to hold opinions without interference

19. The first article of the Universal Declaration of Human Rights recognizes that everyone is “endowed with reason and conscience”, a principle developed further in human rights law to include, among other things, the protection of opinion, expression, belief, and thought. Article 19 (1) of the International Covenant on Civil and Political Rights, also echoing the Universal Declaration, provides that “everyone shall have the right to hold opinions without interference”. Opinion and expression are closely related to one another, as restrictions on the right to receive information and ideas may interfere with the ability to hold opinions, and interference with the holding of opinions necessarily restricts the expression of them. However, human rights law has drawn a conceptual distinction between the two. During the negotiations on the drafting of the Covenant, “the freedom to form an opinion and to develop this by way of reasoning was held to be absolute and, in contrast to freedom of expression, not allowed to be restricted by law or other power”.¹⁰ The ability to hold an opinion freely was seen to be a fundamental element of human dignity and democratic self-governance, a guarantee so critical that the Covenant would allow no interference, limitation or restriction. Consequently, the permissible limitations in article 19 (3) expressly apply only to the right to freedom of expression in article 19 (2). Interference with the right to hold opinions is, by contrast, per se in violation of article 19 (1).

20. Commentators and courts have devoted much less attention to the right to hold opinions than to expression. Greater attention is warranted, however, as the mechanics of holding opinions have evolved in the digital age and exposed individuals to significant vulnerabilities. Individuals regularly hold opinions digitally, saving their views and their search and browse histories, for instance, on hard drives, in the cloud, and in e-mail archives, which private and public authorities often retain for lengthy if not indefinite periods. Civil society organizations likewise prepare and store digitally memoranda, papers and publications, all of which involve the creation and holding of opinions. In other words, holding opinions in the digital age is not an abstract concept limited to what may be in one’s mind. And yet, today, holding opinions in digital space is under attack. Offline, interference with the right to hold an opinion may involve physical harassment, detention or subtler efforts to punish individuals for their opinion (see CCPR/C/78/D/878/1999, annex, paras. 2.5, 7.2 and 7.3). Interference may also include such efforts as targeted surveillance, distributed denial of service attacks, and online and offline intimidation, criminalization and harassment. Targeted digital interference harasses individuals and civil society organizations for the opinions they hold in many formats. Encryption and anonymity enable individuals to avoid or mitigate such harassment.

21. The right to hold opinions without interference also includes the right to form opinions. Surveillance systems, both targeted and mass, may undermine the right to form an opinion, as the fear of unwilling disclosure of online activity, such as search and browsing, likely deters individuals from accessing information, particularly where such surveillance leads to repressive outcomes. For all these reasons, restrictions on encryption and anonymity must be assessed to determine whether they would amount to an impermissible interference with the right to hold opinions.

¹⁰ Manfred Nowak, *UN Covenant on Civil and Political Rights: CCPR Commentary* (1993), p. 441.

C. Right to freedom of expression

22. The right to freedom of expression under article 19 (2) of the International Covenant on Civil and Political Rights expands upon the Universal Declaration's already broad guarantee, protecting the "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice". A significant accumulation of jurisprudence, special procedure reporting, and resolutions within the United Nations and regional human rights systems underscores that the freedom of expression "is essential for the enjoyment of other human rights and freedoms and constitutes a fundamental pillar for building a democratic society and strengthening democracy" (Human Rights Council resolution 25/2). The Human Rights Council, the General Assembly and individual States regularly assert that individuals enjoy the same rights online that they enjoy offline.¹¹ The present report will not repeat all the elements of this consensus. In the context of encryption and anonymity, three aspects of the text deserve particular emphasis (see paras. 23–26 below).

23. **Freedom to seek, receive, and impart information and ideas:** In environments of prevalent censorship, individuals may be forced to rely on encryption and anonymity in order to circumvent restrictions and exercise the right to seek, receive and impart information. Some States have curtailed access with a variety of tools. State censorship, for instance, poses sometimes insurmountable barriers to the right to access information. Some States impose content-based, often discriminatory restrictions or criminalize online expression, intimidating political opposition and dissenters and applying defamation and lese-majesty laws to silence journalists, defenders and activists. A VPN connection, or use of Tor or a proxy server, combined with encryption, may be the only way in which an individual is able to access or share information in such environments.

24. It bears emphasizing that human rights law also protects the right to seek, receive and impart scientific information and ideas. The Universal Declaration and the International Covenant on Economic, Social and Cultural Rights protect rights to education and "to share in scientific advancement and its benefits". Encryption and anonymity technologies enable individuals to share in such information in situations where they are otherwise denied, and they are themselves examples of scientific advancement. Their use empowers individuals to gain access to the benefits of scientific progress that might be curtailed by Government. The Special Rapporteur in the field of cultural rights noted that "the rights to science and to culture should both be understood as including a right to have access to and use information and communication and other technologies in self-determined and empowering ways" (see A/HRC/20/26, para. 19).

25. **Regardless of frontiers:** The major instruments guaranteeing freedom of expression explicitly acknowledge the transboundary scope of the right. Individuals enjoy the right to receive information from, and transmit information and ideas of all kinds to, places beyond their borders.¹² However, some States filter or block data on the basis of keywords, denying access by deploying technologies that rely on access to text. Encryption enables an individual to avoid such filtering, allowing information to flow across borders. Moreover, individuals do not control — and are usually unaware of — how or if their communications cross borders. Encryption and anonymity may protect information of all individuals as it transits through servers located in third countries that filter content.

¹¹ See, e.g., General Assembly resolution 68/167, Human Rights Council resolution 26/13 and Council of Europe recommendation CM/Rec (2014) 6 of the Committee of Ministers to member States on a guide to human rights for Internet users.

¹² The European Court of Human Rights has recognized this point. See *Ahmet Yildirim v. Turkey*, (2012); *Cox v. Turkey*, (2010); *Case of Groppera Radio AG and Others v. Switzerland* (1990).

26. **Through any media:** Articles 19 of the Universal Declaration and the International Covenant on Civil and Political Rights were drafted with the foresight to accommodate future technological advances (A/HRC/17/27). The States parties to the Covenant chose to adopt the general phrase “through any other media” as opposed to an enumeration of then-existing media. Partly on this basis, international mechanisms have repeatedly acknowledged that the protections of freedom of expression apply to activities on the Internet. Regional courts have likewise recognized that protections apply online.¹³ The European Court of Human Rights, in discussing the similar protection of expression in the European Convention for the Protection of Human Rights and Fundamental Freedoms, has indicated that the forms and means through which information is transmitted and received are themselves protected, since any restriction imposed on the means necessarily interferes with the right to receive and impart information.¹⁴ In this sense, encryption and anonymity technologies are specific media through which individuals exercise their freedom of expression.

D. Roles of corporations

27. Corporations in a variety of sectors play roles in advancing or interfering with privacy, opinion and expression, including encryption and anonymity. Much online communication (and virtually all of it in some countries) is carried on networks owned and operated by private corporations, while other corporations own and manage websites with substantial user-generated content. Others are active players in the surveillance and spyware markets, providing hardware and software to Governments to compromise the security of individuals online. Others develop and provide services for secure and private online storage. Telecommunications entities, Internet service providers, search engines, cloud services and many other corporate actors, often described as intermediaries, promote, regulate or compromise privacy and expression online. Intermediaries may store massive volumes of user data, to which Governments often demand access. Encryption and anonymity may be promoted or compromised by each of these corporate actors.

28. A full exploration of the role of corporations to protect their users’ security online is beyond the scope of the present report, which is focused on State obligations. However, it remains important to emphasize that “the responsibility to respect human rights applies throughout a company’s global operations regardless of where its users are located, and exists independently of whether the State meets its own human rights obligations” (see A/HRC/27/37, para. 43). At a minimum, corporations should apply principles such as those laid out in the Guiding Principles on Business and Human Rights, the Global Network Initiative’s Principles on Freedom of Expression and Privacy, the European Commission’s ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights and the Telecommunications Industry Dialogue Guiding Principles, which encourage corporations to commit to protect human rights, undertake due diligence to ensure the positive human rights impact of their work and remediate adverse impacts of their work on human rights. In the future, the Special Rapporteur will focus on the roles

¹³ European Commission of Human Rights, *Neij and Sunde Kolmisoppi v. Sweden*, (2013); European Court of Human Rights, *Perrin v. United Kingdom*, (2005); African Court on Human and Peoples’ Rights, *Zimbabwe Lawyers for Human Rights and Institute for Human Rights and Development (on behalf of Meldrum) v. Zimbabwe* (2009); *Case of Herrera Ulloa v. Costa Rica, Herrera Ulloa v. Costa Rica*, Preliminary Objections, Merits, Reparations and Costs, Series C No. 107, IHRL 1490 (IACHR 2004).

¹⁴ See *Autronic AG v. Switzerland* (1990); *De Haes and Gijssels v. Belgium* (1997), para. 48; *News Verlags GmbH and Co.KG v. Austria* (2000).

corporations should play in preserving individual security to exercise freedom of opinion and expression.

IV. Evaluating restrictions on encryption and anonymity

A. Legal framework

29. The permissible limitations on the right to privacy should be read strictly, particularly in an age of pervasive online surveillance — whether passive or active, mass or targeted — regardless of whether the applicable standards are “unlawful and arbitrary” under article 17 of the International Covenant on Civil and Political Rights, “arbitrary” under article 12 of the Universal Declaration, “arbitrary or abusive” under article 11 of the American Convention on Human Rights, or “necessary in a democratic society” under article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (see A/HRC/13/37, paras. 14–19). Privacy interferences that limit the exercise of the freedoms of opinion and expression, such as those described in this report, must not in any event interfere with the right to hold opinions, and those that limit the freedom of expression must be provided by law and necessary and proportionate to achieve one of a handful of legitimate objectives.

30. No restrictions may be imposed on the right to hold opinions without interference; restrictions under article 19 (3) of the Covenant only apply to expression under article 19 (2). In environments where one’s opinions, however held online, result in surveillance or harassment, encryption and anonymity may provide necessary privacy. Restrictions on such security tools may interfere with the ability of individuals to hold opinions.

31. Restrictions on encryption and anonymity, as enablers of the right to freedom of expression, must meet the well-known three-part test: any limitation on expression must be provided for by law; may only be imposed for legitimate grounds (as set out in article 19 (3) of the Covenant); and must conform to the strict tests of necessity and proportionality.

32. First, for a restriction on encryption or anonymity to be “provided for by law”, it must be precise, public and transparent, and avoid providing State authorities with unbounded discretion to apply the limitation (see Human Rights Committee, general comment No. 34 (2011)). Proposals to impose restrictions on encryption or anonymity should be subject to public comment and only be adopted, if at all, according to regular legislative process. Strong procedural and judicial safeguards should also be applied to guarantee the due process rights of any individual whose use of encryption or anonymity is subject to restriction. In particular, a court, tribunal or other independent adjudicatory body must supervise the application of the restriction.¹⁵

33. Second, limitations may only be justified to protect specified interests: rights or reputations of others; national security; public order; public health or morals. Even where a State prohibits by law “advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence, as provided by Article 20 of the Covenant, any restrictions on expression must be consistent with Article 19(3) (A/67/357). No other grounds may justify restrictions on the freedom of expression. Moreover, because

¹⁵ See International Covenant on Civil and Political Rights, article 2 (3)(b); CCPR/C/79/Add.110, para. 22; the Johannesburg Principles on National Security, Freedom of Expression and Access to Information.

legitimate objectives are often cited as a pretext for illegitimate purposes, the restrictions themselves must be applied narrowly.¹⁶

34. Third, the State must show that any restriction on encryption or anonymity is “necessary” to achieve the legitimate objective.¹⁷ The European Court of Human Rights has concluded appropriately that the word “necessary” in article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms means that the restriction must be something more than “useful,” “reasonable” or “desirable”.¹⁸ Once the legitimate objective has been achieved, the restriction may no longer be applied. Given the fundamental rights at issue, limitations should be subject to independent and impartial judicial authority, in particular to preserve the due process rights of individuals.

35. Necessity also implies an assessment of the proportionality of the measures limiting the use of and access to security online.¹⁹ A proportionality assessment should ensure that the restriction is “the least intrusive instrument amongst those which might achieve the desired result”.²⁰ The limitation must target a specific objective and not unduly intrude upon other rights of targeted persons, and the interference with third parties’ rights must be limited and justified in the light of the interest supported by the intrusion. The restriction must also be “proportionate to the interest to be protected”.²¹ A high risk of damage to a critical, legitimate State interest may justify limited intrusions on the freedom of expression. Conversely, where a restriction has a broad impact on individuals who pose no threat to a legitimate government interest, the State’s burden to justify the restriction will be very high.²² Moreover, a proportionality analysis must take into account the strong possibility that encroachments on encryption and anonymity will be exploited by the same criminal and terrorist networks that the limitations aim to deter. In any case, “a detailed and evidence-based public justification” is critical to enable transparent public debate over restrictions that implicate and possibly undermine freedom of expression (see A/69/397, para. 12).

B. State practice: examples and concerns

36. The trend lines regarding security and privacy online are deeply worrying. States often fail to provide public justification to support restrictions. Encrypted and anonymous communications may frustrate law enforcement and counter-terrorism officials, and they complicate surveillance, but State authorities have not generally identified situations — even in general terms, given the potential need for confidentiality — where a restriction has been necessary to achieve a legitimate goal. States downplay the value of traditional non-digital tools in law enforcement and counter-terrorism efforts, including transnational

¹⁶ See Human Rights Committee, general comment No. 34 on freedom of opinion and expression, para. 30, and general comment No. 31.

¹⁷ See Human Rights Committee, general comment No. 34, para. 2, and communication No. 2156/2012, Views adopted on 10 October 2014.

¹⁸ See *Case of The Sunday Times v. United Kingdom*, judgement of 26 April 1979, para. 59.

¹⁹ See African Court Human and Peoples’ Rights, *Lohe Issa Konate v. Burkina Faso*, application No. 004/2013, paras. 148 and 149 (2014); European Court of Human Rights, *Case of The Sunday Times*, para. 62.

²⁰ See Human Rights Committee, general comment No. 27 (1999) on freedom of movement, para. 14.

²¹ See *ibid.*, para. 14.

²² See Inter-American Commission on Human Rights, OEA /Serv.L/V/II.149, para. 134.

cooperation.²³ As a consequence, the public lacks an opportunity to measure whether restrictions on their online security would be justified by any real gains in national security and crime prevention. Efforts to restrict encryption and anonymity also tend to be quick reactions to terrorism, even when the attackers themselves are not alleged to have used encryption or anonymity to plan or carry out an attack. Moreover, even where the restriction is arguably in pursuit of a legitimate interest, many laws and policies regularly do not meet the standards of necessity and proportionality and have broad, deleterious effects on the ability of all individuals to exercise freely their rights to privacy and freedom of opinion and expression.

37. It also bears noting that the United Nations itself has not provided strong communication security tools to its staff or to those who would visit United Nations websites, making it difficult for those under threat to securely reach the United Nations, human rights mechanisms online.²⁴

1. Encryption

38. Some Governments seek to protect or promote encryption to ensure the privacy of communications. For instance,²⁵ the Marco Civil da Internet Law of Brazil, adopted in 2014, guarantees the inviolability and secrecy of user communications online, permitting exceptions only by court order. The E-Commerce Act and Telecommunication Act of Austria do not restrict encryption, and the Government has undertaken public awareness campaigns to educate the public about digital security. Greek law and regulations promote the effective use of both encryption and anonymity tools. Germany, Ireland and Norway permit and promote the use of encryption technologies and oppose any efforts to weaken encryption protocols. Similarly, Swedish and Slovak laws do not restrict the use of encryption online. The United States of America encourages the use of encryption, and the United States Congress should further consider a secure data act introduced in the Congress that would prohibit the Government from requiring companies to weaken product security or insert back-door access measures. Several Governments fund efforts to share or train in the use of encryption and anonymity technologies to help individuals evade censorship and protect their security online, including Canada, the Netherlands, Sweden, the United Kingdom of Great Britain and Northern Ireland and the United States. In addition, export regulations should facilitate the transfer of encryption technologies wherever possible. Although the present report does not provide an overall legal assessment of all national approaches to encryption, these noted elements — non-restriction or comprehensive protection, the requirement of court orders for any specific limitation, and public education — deserve wider application as means to protect and promote the rights to freedom of opinion and expression.

39. Nonetheless, the regulation of encryption often fails to meet freedom of expression standards in two leading respects. First, restrictions have generally not been shown to be necessary to meet a particular legitimate interest. This is especially the case given the breadth and depth of other tools, such as traditional policing and intelligence and transnational cooperation, that may already provide substantial information for specific law enforcement or other legitimate purposes. Second, they disproportionately impact the rights

²³ But see Centre for International Governance Innovation and Chatham House, *Toward a Social Compact for Digital Privacy and Security: Statement by the Global Commission on Internet Governance* (2015).

²⁴ For instance, staff of the Office of the United Nations High Commissioner for Human Rights (OHCHR) in Geneva do not have access to end-to-end e-mail encryption, and the OHCHR website is not encrypted.

²⁵ Many examples in this paragraph are taken from the relevant government submissions.

to freedom of opinion and expression enjoyed by targeted persons or the general population.

Bans on encryption for individual use

40. Outright prohibitions on the individual use of encryption technology disproportionately restrict the freedom of expression, because they deprive all online users in a particular jurisdiction of the right to carve out private space for opinion and expression, without any particular claim of the use of encryption for unlawful ends.

41. State regulation of encryption may be tantamount to a ban, such as rules (a) requiring licences for encryption use; (b) setting weak technical standards for encryption; and (c) controlling the import and export of encryption tools. By limiting encryption tools to government-approved standards and controlling the import or export of encryption technologies, States ensure encryption software maintains weaknesses that allow Governments to access the content of communications. For example, while the law may be in flux, India has provided that service providers may not deploy “bulk encryption” on their networks, while the law has also restricted individuals from using encryption greater than an easily breakable 40-bit key length without prior permission and required anyone using stronger encryption to provide the Government with a copy of the encryption keys.²⁶ Reports indicate that encryption products in China may be required to adhere to government-approved encryption algorithms that have not been peer-reviewed for security.²⁷ The Pakistan Telecommunication Authority requires prior approval for the use of VPNs and encryption.²⁸ Cuba requires regulatory authorization for those using encryption.²⁹ In Ethiopia, the Government has the power to set the technical standards of encryption and recently enacted regulation that criminalizes the manufacture, assembly or import of any telecommunications equipment without a permit.³⁰ Such regulations impermissibly interfere with the individual use of encryption in communications.

Intentional weakening of encryption

42. Some States have implemented or proposed implementing so-called back-door access in commercially available products, forcing developers to install weaknesses that allow government authorities access to encrypted communications. Some Governments have developed or purchased tools to allow such access for domestic surveillance purposes.³¹ Senior officials in the United Kingdom and the United States appear to advocate requiring back-door access.³² States supporting such measures often claim that a legal framework for back-door access is necessary to intercept the content of encrypted communications. Governments proposing back-door access, however, have not

²⁶ Government of India, Ministry of Communications and IT, Licence Agreement for Provision of Internet Services, (2007). Available from http://dot.gov.in/sites/default/files/internet-licence-dated%2016-10-2007_0.pdf. See especially sect. 2.2 (vii).

²⁷ See, e.g., Counter-terrorism Law, art. 15 (initial draft of 8 November 2014). Available from <http://chinalawtranslate.com/en/ctldraft/>.

²⁸ See www.ispak.pk/Downloads/PTA_VPN_Policy.pdf.

²⁹ Submission of Cuba.

³⁰ See Ethiopia Telecom Fraud Offence Proclamation 761/2012, sects. 3–10.

³¹ See Morgan Maquis-Boire and others, *For Your Eyes Only* (2013, Citizen Lab).

³² See the speech given by Prime Minister David Cameron on 12 January 2015 at the Conservative Party pledges conference for the 2015 general election and the speech given by James Comey, Director of the Federal Bureau of Investigation, on 16 October 2014, entitled “Going dark: are technology, privacy and public safety on a collision course?”, at the Brookings Institution, Washington, D.C.

demonstrated that criminal or terrorist use of encryption serves as an insuperable barrier to law enforcement objectives. Moreover, based on existing technology, intentional flaws invariably undermine the security of all users online, since a backdoor, even if intended solely for government access, can be accessed by unauthorized entities, including other States or non-State actors. Given its widespread and indiscriminate impact, back-door access would affect, disproportionately, all online users.

43. The debate on this issue highlights a critical point: requiring encryption back-door access, even if for legitimate purposes, threatens the privacy necessary to the unencumbered exercise of the right to freedom of expression. Back-door access has practical limitations; the exploitation of intentional weaknesses could render encrypted content susceptible to attack, even if access is provided with the sole intention of allowing government or judicial control. Governments certainly face a dilemma when their obligation to protect freedom of expression is in conflict with their obligations to prevent violations of the right to life or bodily integrity, which are put at risk by terrorism and other criminal behaviour. But other recourses are available to States to request the disclosure of encrypted information, such as through judicial warrants. In such situations, States must demonstrate that general limitations on the security provided by encryption would be necessary and proportionate. States must show, publicly and transparently, that other less intrusive means are unavailable or have failed and that only broadly intrusive measures, such as backdoors, would achieve the legitimate aim. Regardless, measures that impose generally applicable restrictions on massive numbers of persons, without a case-by-case assessment, would almost certainly fail to satisfy proportionality.

Key escrows

44. A key escrow system permits individual access to encryption but requires users to store their private keys with the Government or a “trusted third party”. Key escrows, however, have substantial vulnerabilities. For instance, the key escrow system depends on the integrity of the person, department or system charged with safeguarding the private keys, and the key database itself could be vulnerable to attack, undermining any user’s communication security and privacy. Key escrow systems, rejected (along with back-door access) after significant debate in the United States in the so-called Crypto Wars of the 1990s, are currently in place in several countries and have been proposed in others. In 2011, Turkey passed regulations requiring encryption suppliers to provide copies of encryption keys to government regulators before offering their encryption tools to users.³³ The vulnerabilities inherent in key escrows render them a serious threat to the security to exercise the freedom of expression.

Mandatory key disclosure versus targeted decryption orders

45. In a situation where law enforcement or national security arguments may justify requests for access to communications, authorities may see two options: order either decryption of particular communications or, because of a lack of confidence that a targeted party would comply with a decryption order, disclosure of the key necessary for decryption. Targeted decryption orders may be seen as more limited and less likely to raise proportionality concerns than key disclosure, focusing on specific communications rather than an individual’s entire set of communications encrypted by a particular key. Key disclosure, by contrast, could expose private data well beyond what is required by the exigencies of a situation.³⁴ Moreover, key disclosure or decryption orders often force

³³ Law No. 5651 on Regulating Broadcasting in the Internet and Fighting against Crimes Committed through Internet Broadcasting.

³⁴ The European Commission Counter-Terrorism Coordinator has urged consideration of mandatory key

A/HRC/29/32

corporations to cooperate with Governments, creating serious challenges that implicate individual users online. Key disclosure exists by law in a number of European countries.³⁵ In both cases, however, such orders should be based on publicly accessible law, clearly limited in scope focused on a specific target, implemented under independent and impartial judicial authority, in particular to preserve the due process rights of targets, and only adopted when necessary and when less intrusive means of investigation are not available. Such measures may only be justified if used in targeting a specific user or users, subject to judicial oversight.

Legal presumptions

46. Some States may identify the mere use of encryption technologies as illicit behaviour. For instance, charges against the Zone 9 blogger collective in Ethiopia included suggestions that the mere training in communication security was evidence of criminal behaviour.³⁶ Such presumptions fail to meet the standards for permissible restrictions. Similarly, States undermine the rights to privacy and freedom of expression when they penalize those who produce and distribute tools to facilitate online access for activists.

2. Anonymity

47. Anonymity has been recognized for the important role it plays in safeguarding and advancing privacy, free expression, political accountability, public participation and debate.³⁷ The Universal Declaration and the International Covenant on Civil and Political Rights do not address anonymity. During negotiation of the Covenant, it was proposed to include in article 19 (1) the phrase, “anonymity is not permitted”. However, this was rejected “on the grounds, among others, that anonymity might at times be necessary to protect the author” and “that such a clause might prevent the use of pen names”.³⁸ The Special Rapporteur on Freedom of Expression of the Inter-American Commission on Human Rights found that “the right to freedom of thought and expression and the right to private life protect anonymous speech from government restrictions”.³⁹ Several States enjoy long traditions of celebrating anonymity in their political cultures, but very few provide general protection in law for anonymous expression. Some States exert significant pressure against anonymity, offline and online. Yet because anonymity facilitates opinion and expression in significant ways online, States should protect it and generally not restrict the technologies that provide it. Several States’ judiciaries have protected anonymity, at least in limited instances. For instance, the Supreme Court of Canada recently struck down the warrantless acquisition of anonymous user identity online.⁴⁰ The Constitutional Court of the Republic of Korea struck down anti-anonymity laws as unconstitutional.⁴¹ The Supreme

disclosure. See Council of the European Union, General Secretariat, meeting document D1035/15 (2015).

³⁵ See, e.g., United Kingdom, Regulation of Investigatory Powers Act (mandatory key disclosure); France, Law No. 2001-1062 (disclosure of encryption keys on authorization by a judge); Spain, Law on Telecommunications 25/2007 (key disclosure).

³⁶ See <http://trialtrackerblog.org/2014/07/19/contextual-translation-of-the-charges-of-the-zone9-bloggers/>.

³⁷ See, e.g., Inter-American Commission on Human Rights, OEA /Serv.L/V/II.149, para. 134; United States, *McIntyre v. Ohio Elections Commission* (1995); Lord Neuberger, speech to RB Conference on the Internet, entitled, “What’s a name? Privacy and Anonymous Speech on the Internet” (2014).

³⁸ Marc J. Bossuyt, *Guide to the “Travaux Préparatoires” of the International Covenant on Civil and Political Rights* (1987), pp. 379-80.

³⁹ See Organization of American States, press release 17/15.

⁴⁰ *R. v. Spencer* (2014).

⁴¹ Decision 2010 Hun-Ma 47, 252 (consolidated) announced 28 August 2012.

Court of the United States has consistently protected the right to anonymous expression.⁴² The European Court of Human Rights has recognized anonymity as important to the freedom of expression but permits limitations in cases where necessary to achieve legitimate objectives.

48. Many States recognize the lawfulness of maintaining the anonymity of journalists' sources. The Mexican Supreme Court and Mexican Code of Criminal Procedures recognize the right of journalists to maintain the anonymity of their sources; yet pressures on journalists are in fact severe.⁴³ The Constitutions of Argentina, Brazil, Ecuador and Paraguay explicitly protect sources; Chile, El Salvador, Panama, Peru, Uruguay and Venezuela (Bolivarian Republic of) protect sources in law.⁴⁴ The Mozambique Constitution protects sources, while Angola purports to do so by statute.⁴⁵ Australia, Canada, Japan and New Zealand have established case-specific judicial balancing tests to analyse source protection, although pressure on journalists may undermine such protections over time.⁴⁶ States often breach source anonymity in practice, even where it is provided for in law.

Prohibition of anonymity

49. Prohibition of anonymity online interferes with the right to freedom of expression. Many States ban it regardless of any specific government interest. The Constitution of Brazil (art. 5) prohibits anonymous speech. The Constitution of the Bolivarian Republic of Venezuela (art. 57) similarly prohibits anonymity. In 2013, Viet Nam outlawed the use of pseudonyms, which forced individuals with personal blogs to publicly list their real name and address.⁴⁷ In 2012, the Islamic Republic of Iran required the registration of all IP addresses in use inside the country and cybercafe users to register their real names before using a computer.⁴⁸ Ecuadoran law requires commenters on websites and mobile phone owners to register under a real name.⁴⁹

50. Certain States have passed laws that require real-name registration for online activity, a kind of ban on anonymity. In the Russian Federation, bloggers with 3,000 or more daily readers must register with the media regulator and identify themselves publicly, and cybercafe users reportedly must provide identification to connect to public wireless facilities.⁵⁰ China reportedly announced regulations requiring Internet users to register real

⁴² *McIntyre v. Ohio Elections Commission* (1995), pp. 342 and 343.

⁴³ See new Federal Code of Criminal Procedures, art. 244.

⁴⁴ See Argentina, Constitution, art. 43; Brazil, Constitution, title II, chap. I, art. 5, XIV; Ecuador, Constitution, art. 20; Paraguay, Constitution, art. 29 (1). See also Chile, Law 19,733; El Salvador, Criminal Procedure Code; Panama, Law 67, art. 21; Peru, Criminal Procedure Code; Uruguay, Law 16,099; Bolivarian Republic of Venezuela, Law for Journalism 4.819, art. 8.

⁴⁵ See Mozambique, Constitution, art. 48(3); Angola, Press Law 7/06, art. 20(1).

⁴⁶ Australia Evidence Amendment (Journalists' Privilege) Act 2007; Canada, Court of Queen's Bench of Alberta, *Wasylshen v. Canadian Broadcasting Corporation* (2005); Japan, Case 2006 (Kyo) No. 19 (2006); New Zealand Evidence Act, sect. 68 (2006).

⁴⁷ Human Rights Watch, "Vietnam: new decree punishes press", 23 February, 2011; Freedom House, "Vietnam: freedom of the press", 2012; Article 19, Comment on Decree No. 02 of 2011 on Administrative Responsibility for Press and Publication Activities of the Prime Minister of the Socialist Republic of Vietnam (June 2011).

⁴⁸ Islamic Republic of Iran, Bill 106, Communication Regulation Authority.

⁴⁹ See Ecuador, Organic Law on Communications (2013).

⁵⁰ Bill No. 428884-6 amending the Federal Law on Information, Information Technologies and Protection of Information and a number of legislative acts of the Russian Federation on streamlining the exchange of information with the use of information and telecommunication networks; Reuters, "Russia Demands Internet Users Show ID to Access Public Wifi," 8 August 2014.

names for certain websites and avoid spreading content that challenges national interests.⁵¹ South Africa also requires real name registration for online and mobile telephone users.⁵²

51. Likewise, Governments often require SIM card registration; for instance, nearly 50 countries in Africa require or are in the process of requiring the registration of personally identifiable data when activating a SIM card.⁵³ Colombia has had a mandatory mobile registration policy since 2011, and Peru has associated all SIM cards with a national identification number since 2010.⁵⁴ Other countries are considering such policies. Such policies directly undermine anonymity, particularly for those who access the Internet only through mobile technology. Compulsory SIM card registration may provide Governments with the capacity to monitor individuals and journalists well beyond any legitimate government interest.

52. States have also attempted to combat anonymity tools, such as Tor, proxies and VPNs, by denying access to them. China has long blocked access to Tor,⁵⁵ and Russian government officials reportedly offered more than \$100,000 for techniques to identify anonymous users of Tor.⁵⁶ In addition, Ethiopia,⁵⁷ Iran (Islamic Republic of)⁵⁸ and Kazakhstan⁵⁹ have reportedly sought to block Tor traffic. Because such tools may be the only mechanisms for individuals to exercise freedom of opinion and expression securely, access to them should be protected and promoted.

Restrictions during public unrest

53. Anonymous speech has been necessary for activists and protestors, but States have regularly attempted to ban or intercept anonymous communications in times of protest. Such attempts to interfere with the freedom of expression unlawfully pursue an illegitimate objective of undermining the right to peaceful protest under the Universal Declaration and the International Covenant on Civil and Political Rights.

Intermediary liability

54. Some States and regional courts have moved towards imposing responsibilities on Internet service providers and media platforms to regulate online comments by anonymous users. Ecuador, for instance, in its Organic Communications Law, requires intermediaries to generate mechanisms to record personal data to allow the identification of those posting comments. In *Delfi v. Estonia* (application No. 64569/09), the European Court of Human Rights upheld an Estonian law that imposes liability on a media platform for anonymous defamatory statements posted on its site. Such intermediary liability is likely to result either in real-name registration policies, thereby undermining anonymity, or the elimination of posting altogether by those websites that cannot afford to implement screening procedures,

⁵¹ China Copyright and Media, Internet User Account Name Management Regulations, article 5 (2015).

⁵² South Africa, Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2003; see also Electronic Communications and Transactions Act of 2002 (requiring real name registration for service providers).

⁵³ Kevin P. Donovan and Aaron K. Martin, "The Rise of African SIM Registration", 3 February 2014.

⁵⁴ See Colombia, Decree 1630 of 2011; Perú 21, *Los celulares de prepago en la mira*, 27 May 2010.

⁵⁵ MIT Technology Review, *How China Blocks the Tor Anonymity Network*, 4 April 2012.

⁵⁶ The original offer is available from <http://zakupki.gov.ru/epz/order/notice/zkk44/view/common-info.html?regNumber=0373100088714000008>.

⁵⁷ Runa Sandvik, Ethiopia Introduces Deep Packet Inspection, The Tor Blog (31 May 2012); see also Article 19, 12 January 2015.

⁵⁸ "Phobos", "Iran partially blocks encrypted network traffic", The Tor Blog (10 February 2012).

⁵⁹ "Phobos", "Kazakhstan upgrades censorship to deep packet inspection", The Tor Blog (16 February 2012).

thus harming smaller, independent media. The recently adopted Manila Principles on Intermediary Liability, drafted by a coalition of civil society organizations, provide a sound set of guidelines for States and international and regional mechanisms to protect expression online.

Data retention

55. Broad mandatory data retention policies limit an individual's ability to remain anonymous. A State's ability to require Internet service and telecommunications providers to collect and store records documenting the online activities of all users has inevitably resulted in the State having everyone's digital footprint. A State's ability to collect and retain personal records expands its capacity to conduct surveillance and increases the potential for theft and disclosure of individual information.

V. Conclusions and recommendations

56. Encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age. Such security may be essential for the exercise of other rights, including economic rights, privacy, due process, freedom of peaceful assembly and association, and the right to life and bodily integrity. Because of their importance to the rights to freedom of opinion and expression, restrictions on encryption and anonymity must be strictly limited according to principles of legality, necessity, proportionality and legitimacy in objective. The Special Rapporteur therefore recommends the following.

A. States

57. States should revise or establish, as appropriate, national laws and regulations to promote and protect the rights to privacy and freedom of opinion and expression. With respect to encryption and anonymity, States should adopt policies of non-restriction or comprehensive protection, only adopt restrictions on a case-specific basis and that meet the requirements of legality, necessity, proportionality and legitimacy in objective, require court orders for any specific limitation, and promote security and privacy online through public education.

58. Discussions of encryption and anonymity have all too often focused only on their potential use for criminal purposes in times of terrorism. But emergency situations do not relieve States of the obligation to ensure respect for international human rights law. Legislative proposals for the revision or adoption of restrictions on individual security online should be subject to public debate and adopted according to regular, public, informed and transparent legislative process. States must promote effective participation of a wide variety of civil society actors and minority groups in such debate and processes and avoid adopting such legislation under accelerated legislative procedures. General debate should highlight the protection that encryption and anonymity provide, especially to the groups most at risk of unlawful interferences. Any such debate must also take into account that restrictions are subject to strict tests: if they interfere with the right to hold opinions, restrictions must not be adopted. Restrictions on privacy that limit freedom of expression — for purposes of the present report, restrictions on encryption and anonymity — must be provided by law and be necessary and proportionate to achieve one of a small number of legitimate objectives.

A/HRC/29/32

59. States should promote strong encryption and anonymity. National laws should recognize that individuals are free to protect the privacy of their digital communications by using encryption technology and tools that allow anonymity online. Legislation and regulations protecting human rights defenders and journalists should also include provisions enabling access and providing support to use the technologies to secure their communications.

60. States should not restrict encryption and anonymity, which facilitate and often enable the rights to freedom of opinion and expression. Blanket prohibitions fail to be necessary and proportionate. States should avoid all measures that weaken the security that individuals may enjoy online, such as backdoors, weak encryption standards and key escrows. In addition, States should refrain from making the identification of users a condition for access to digital communications and online services and requiring SIM card registration for mobile users. Corporate actors should likewise consider their own policies that restrict encryption and anonymity (including through the use of pseudonyms). Court-ordered decryption, subject to domestic and international law, may only be permissible when it results from transparent and publicly accessible laws applied solely on a targeted, case-by-case basis to individuals (i.e., not to a mass of people) and subject to judicial warrant and the protection of due process rights of individuals.

B. International organizations, private sector and civil society

61. States, international organizations, corporations and civil society groups should promote online security. Given the relevance of new communication technologies in the promotion of human rights and development, all those involved should systematically promote access to encryption and anonymity without discrimination. The Special Rapporteur urgently calls upon entities of the United Nations system, especially those involved in human rights and humanitarian protection, to support the use of communication security tools in order to ensure that those who interact with them may do so securely. United Nations entities must revise their communication practices and tools and invest resources in enhancing security and confidentiality for the multiple stakeholders interacting with the Organization through digital communications. Particular attention must be paid by human rights protection mechanisms when requesting and managing information received from civil society and witnesses and victims of human rights violations.

62. While the present report does not draw conclusions about corporate responsibilities for communication security, it is nonetheless clear that, given the threats to freedom of expression online, corporate actors should review the adequacy of their practices with regard to human right norms. At a minimum, companies should adhere to principles such as those laid out in the Guiding Principles on Business and Human Rights, the Global Network Initiative's Principles on Freedom of Expression and Privacy, the European Commission's ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights, and the Telecommunications Industry Dialogue Guiding Principles. Companies, like States, should refrain from blocking or limiting the transmission of encrypted communications and permit anonymous communication. Attention should be given to efforts to expand the availability of encrypted data-centre links, support secure technologies for websites and develop widespread default end-to-end encryption. Corporate actors that supply technology to undermine encryption and anonymity should be especially transparent as to their products and customers.

63. The use of encryption and anonymity tools and better digital literacy should be encouraged. The Special Rapporteur, recognizing that the value of encryption and anonymity tools depends on their widespread adoption, encourages States, civil society organizations and corporations to engage in a campaign to bring encryption by design and default to users around the world and, where necessary, to ensure that users at risk be provided the tools to exercise their right to freedom of opinion and expression securely.

Exhibit Y

October 23 2010 - SATURDAY Official Gazette Number: 27738

Information and Communication Technologies Authority:

**BY LAW ON THE PROCEDURES AND PRINCIPLES OF ENCODED OR ENCRYPTED
COMMUNICATION BETWEEN PUBLIC AUTHORITIES AND ORGANIZATIONS
AND REAL AND LEGAL PERSONS IN ELECTRONICAL COMMUNICATION
SERVICE**

CHAPTER ONE

Purpose, Scope, Basis and Definitions

Purpose

ARTICLE 1 – (1) The purpose of this Regulation is to determine the procedures and principles along with the work and transactions to be performed in creation, principles of application, evaluation, approval transactions, security and preservation precautions, auditing, sanctions and recording of the encoded or encrypted communication system between public authorities and organizations and real and legal persons inside electronical communication service according to Law on Electronical Communication number 5809 dated 5/11/2008.

Scope

ARTICLE 2 – (1) This Regulation includes all public authorities and organizations and real and legal persons except for Turkish Armed Forces, General Commandership of Gendarmerie, Coast Guard Commandership, Undersecretariat of National Intelligence Agency, General Directorate of Security and Ministry of Foreign Affairs authorized to have encoded or encrypted communication within electronical communication service and public authorities and organizations and real and legal persons that encoded or encrypted communication systems of these organizations are used.

(2) Authority approved wireless devices and systems determined in Authority regulations that work in output powers and frequency bands assigned for special purposes, to which frequency assignment is not needed to operate are outside the scope of this Regulation.

Basis

ARTICLE 3 – (1) This Regulation has been prepared based on article 39 of Law on Electronical Communication number 5809 dated 5/11/2008.

Definitions

ARTICLE 4 – (1) The following concepts in this Regulation are defined as follows;

a) Specialized organizations : The institutes, universities or organizations that carry out scientific research and development works with whom protocols were made on the subject of encoded or encrypted electronical communication systems,

b) Operator : The company that provides electronical communication service within the frameworks of authorization and / or the electronical communication network and operates the infrastructure,

c) Authority : Information and Communication Technologies Authority,

d) Encryption : The encryption of the messages for the purposes of safe data transfer and preservation,

e) Encryption Algorithm : All mathematical functions and protocols used in encryption, decoding, identity verification and similar other steps of cryptographic transactions,

- f) Encryption Key : The set of variable characters used in encryption and decryption of the data and applied to the algorithm,
- g) Encrypted electronical communication : Communication performed by using encryption techniques with encrypted electronical communication devices,
- h) Encrypted electronical communication device : Wired or wireless electronical communication device used with internal and / or external software and hardware based encryption element,
- i) Encoded communication : The transmission of messages in a changed way according to a priorly agreed code in order for the communication not to be understood by third parties,
- j) National encryption device : Devices developed and produced by Turkish citizens with National Encryption Clearance Certificate in organizations authorized to produce by Ministry of National Defence, and which the security level of cryptographical algorithm, protocol and key management systems are approved by an authorized public authority,
- k) Wireless : Systems used to receive and transmit sounds, data, clearly encoded or encrypted via electromagnetic waves without a physical connection, or just transmit or just receive those,
- l) Manufacturer : Real or legal person manufacturing, adapting or presenting himself as the manufacturer of the electronical communication device by putting his distinctive signature or commercial trade mark, in the case that manufacturer is foreign, the importer and / or authorized representative of the manufacturer, real or legal person who contributes to the chain of sale and / or supply of the device and whose activities affect the features of the device related to security.

CHAPTER TWO

Application, Evaluation, Permission Transactions, Security and Preservation Precautions for Encoded or Encrypted Electronical Communication Services

Application

ARTICLE 5 – (1) All public authorities and organizations along with real and legal persons except for the exceptional authorities stated in Law number 5809 can use encoded and / or encrypted communication as long as it is not in violation of the provisions of this Regulation.

(2) The import or manufacturing of encoded or encrypted communication device / system is performed by the manufacturer. Manufacturer,

applies to the Authority in order to get permission for the devices / systems to be manufactured or imported with;

- a) Permission application letter,
- b) Two signed copies of related Authority Application Form filled by owner of the request taking into consideration the features and type of communication system (land, sea, air, satellite) to be established,
- c) Documents on the encryption technique / device to be used and technical features of the electronical communication system that will be used,
- d) Encryption algorithm and key, key production, distribution and installation module / device, all software / hardware used for this purpose, software and / or hardware making it possible to decrypt the code when necessary,
- e) If there are two samples of the device, optional softwares / hardwares, accessories, special

2/5

apparatus to be used in testing of these devices when necessary,

f) Chamber of Commerce Certificate, Chamber of Industry Certificate, copy of Commercial Registration Gazette, charter or similar operating certificate for real and legal persons,

g) List of authorized signatures to represent the real and legal persons,

h) Record of previous convictions for authorized representatives of legal persons and real persons,

i) The technical document content stated in Attachment – 2 of Regulation for Wireless and Telecommunication Terminal Equipments (1999/5/AT) published in Official Gazette dated 24/3/2007 and number 26472 for devices within the scope of this Regulation.

Evaluation

ARTICLE 6 – (1) The applications of electronical communication service device / system manufacturers are evaluated according to Regulation on Procedures and Principles On Wireless Transactions published in Official Gazette with number 27291 on the date 17/7/2009 in terms of wireless systems; and according to Regulation on Wireless and Telecommunication Terminal Equipments (1999/5/AT) in stages of presentation to the market, distribution, existence in market and presentation to service.

(2) In the case that there is a sentence for crimes against the inseparable integrity of the Government with country and nation, fundamental principles of Republic, Constitutional order and operation of this order, national defence, Government confidential information and spying, debt, malversation, bribery, theft, cheating, breach of confidence, rigging an auction, rigging the execution of an activity, laundering of assets value from crime or trafficking or any crime within the scope of Law on Combat Against Terrorism number 3713 dated 12/4/1991, by the manufacturer or a person who has authorized signature representation of the manufacturing company, the application will be rejected.

(3) In the case that public authorities or organizations and real and legal persons who bring with travellers or in absolute return or import individually or bring by mail, encoded or encrypted communication device / systems hand in the encoding or encryption keys for these devices / systems to the Authority, the use and installation may be permitted. Encoded or encrypted communications detected to be done without Authority's permission will be closed to communication and a criminal complaint will be submitted about related persons.

(4) Encoded or encrypted device / system applications that are not seen appropriate to the related legislation will be rejected in applications done by the manufacturer.

(5) In the case that it is seen necessary by the Authority, cooperation with specialized organizations related to encoded or encrypted electronical communication systems will be established.

(6) All transactions related to the installation and operation of encoded or encrypted electronical communication systems by foreign states in order to establish communication limited to their government headquarters and diplomatic representation offices in Turkey or to be used for purposes of their own domestic security will be evaluated by Ministry of Foreign Affairs according to principles of mutuality.

(7) The principle in encoded or encrypted communication systems used by public authorities and organizations, is the use of national encryption devices designed and manufactured in Turkey.

Permission

ARTICLE 7 – (1) Applications for encoded or encrypted electronical communication services are evaluated by the Authority. In the case that the application is approved, code or encryption will be delivered to the Authority and permission may be given to the manufacturer.

(2) Permission is not needed for systems of encoded or encrypted communication inside local areas such as building, storage areas, garages that does not use an electronical communication system infrastructure operated by an operator.

(3) Manufacturers, public authorities and organizations along with real and legal persons can not make any changes or repairs on the basis of hardware and software on technical features of the devices / systems without a permission from the Authority related to the encoded or encrypted electronical communication systems they possess. Any change or repair action can only be done with the approval of the Authority. In the case of a detection of any change or repair in technical features of devices / systems, the device / system will be closed to communication and criminal complaint will be submitted about related persons.

Security and preservation measures

ARTICLE 8 – (1) All public authorities and organizations along with real and legal persons that install and operate encoded or encrypted electronical communication devices / systems will take necessary preservation precautions to prevent the unauthorized use and possession of the systems by unauthorized persons.

(2) Code or encryption algorithm and keys belonging to the encoded or encrypted electronic communication devices / systems to be delivered to the Authority by Manufacturers will be preserved by the Authority.

CHAPTER THREE

Audition, Sanctions and Recording

Audition

ARTICLE 9 – (1) The fulfillment of the requirements of the permissions given with responsibilities and regulated in this Regulation by public authorities and organizations along with real and legal persons will be audited within the frameworks of article 59 of Law number 5809.

(2) In sea authority areas, the audition is performed by Coast Guard Commandership in coordination with the Authority.

Sanctions

ARTICLE 10 – (1) In the case of violation of the provisions of this Regulation, articles 60 and 63 of Law number 5809 will be applied for users and manufacturers of encoded or encrypted electronical communication device / system.

Recording

ARTICLE 11 – (1) Manufacturer will submit the device information (trademark, model, serial number, device type, International Mobile Equipment Identity (IMEI) number and Tip Authorization Code (TAC) number) presented to the market belonging to public authorities and organizations along with real and legal persons to the Authority in electronical environment and in written form by the last business day of the month following the month of the transaction performed.

CHAPTER FOUR

Various and Final Provisions

Repealed Regulation

ARTICLE 12 – (1) Regulation on Encrypted Wireless Systems published in Official Gazette number 25394 on the date 6/3/2004 has been repealed.

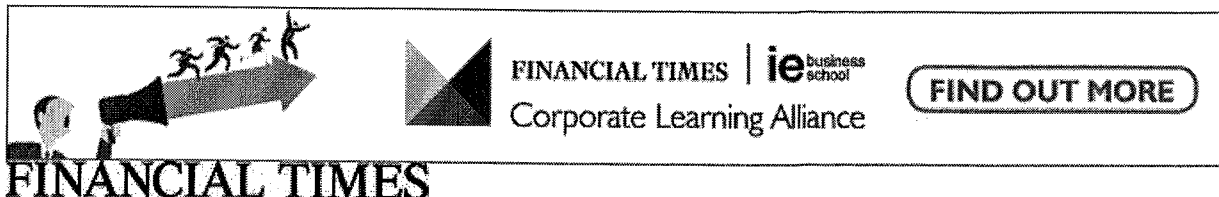
Enforcement

ARTICLE 13 – (1) This Regulation shall enter into force on the date of publication of the Regulation.

Execution

ARTICLE 14 – (1) The provisions of this Regulation are executed by President of Council of Information and Communication Technologies.

Exhibit Z



FINANCIAL TIMES | ie business school
Corporate Learning Alliance

FIND OUT MORE

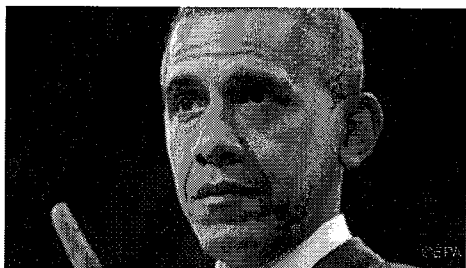
FINANCIAL TIMES

March 3, 2015 6:48 am

Obama seeks reboot of China cyber laws

Tom Mitchell in Beijing

Share Author alerts Print Clip Comments



US President Barack Obama has lashed out at new Chinese cyber security regulations, elevating the increasingly contentious issue to the top of the two countries' bilateral agenda.

"This is something that I've raised with President Xi [Jinping]," Mr Obama said in an interview with Reuters. "We have made it very clear to them that this is something they are going to have to change if they are to do business with the United States."

Over recent weeks, US and European corporate executives have expressed alarm over two new pieces of Chinese legislation targeting telecom companies, internet service providers and banks. Both are still in the drafting process, but could begin to take effect this month.

Business lobby groups have asked the Obama administration and the European Commission to raise the issue in bilateral trade talks with Beijing. They suspect that the new rules, which Chinese government officials say are needed to address legitimate national security concerns, are in fact aimed at boosting China's own tech companies.

Four US cabinet secretaries have written a letter to their Chinese counterparts about the issue, according to people familiar with the diplomatic exchange. In a statement last week, US trade representative Michael Froman also argued that the new regulations "go directly against a series of China's bilateral and multilateral trade commitments".

Mr Obama expressed concern about a draft Chinese antiterrorism law that would force telecom and internet companies to provide Beijing with "back doors" into their systems — as well as require them to store data in China.

China's telecom market is dominated by large state companies that can already be trusted to turn over information demanded by Beijing's security agencies but multinationals also use foreign

providers for private networks and other services.

A separate set of regulations, drafted by the China Banking Regulatory Commission and Ministry of Industry and Information Technology, will require more than 70 per cent of banks' information technology equipment to be "secure and controllable" by 2019.

Under the new guidelines, financial institutions will have to begin informing authorities about their compliance procedures as soon as March 15.

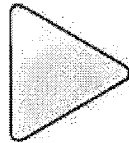
On Tuesday a spokesperson for Beijing's foreign affairs ministry said the laws were China's internal affair.

"We hope the US can regard and manage this correctly, calmly and objectively," he said. "Every country takes measures to protect itself and information security. This should not be criticised."

RELATED TOPICS US trade, China, European Commission, Barack Obama, China Politics & Policy

Share Author alerts Print Clip Comments

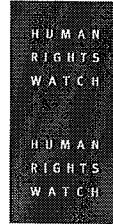
VIDEOS



The carousel contains three video thumbnails:

- Thumbnail 1:** Labeled "FT COMMENT". Title: "What Trump would do as US president".
- Thumbnail 2:** Labeled "First FT IN 60 SECONDS". Title: "FirstFT — Trump and Clinton's Super Tuesday, grey hair".
- Thumbnail 3:** Labeled "FT WORLD". Title: "Myanmar — A life-and-death land battle".

Exhibit AA



JANUARY 20, 2015

China: Draft Counterterrorism Law a Recipe for Abuses

Major Overhaul Needed for Law to Conform with International Legal Obligations

(New York) – The Chinese government should radically revise its **proposed legislation on counterterrorism** to make it consistent with international law and the protection of human rights. The draft law was made public for consultation in November 2014 and is expected to be adopted in 2015 after minimal revisions.

As currently drafted, the law would legitimate ongoing human rights violations and facilitate future abuses, especially in an environment lacking basic legal protections for criminal suspects and a history of gross human rights abuses committed in the name of counterterrorism. Such violations are evident across the country and particularly in the Xinjiang Uyghur Autonomous Region, the region that has been most affected by acts of terrorism and political violence in recent years.

“China has seen appalling attacks on people, and the government has a duty to respond and protect the population,” said **Sophie Richardson**, China director at Human Rights Watch. “But in its present form this law is little more than a license to commit human rights abuses. The draft needs to be completely overhauled and brought in line with international legal standards.”

The Chinese government claims that its proposed counterterrorism legislation responds to and conforms with United Nations Security Council resolutions urging countries to take measures to combat and strengthen their cooperation against terrorism. Yet such resolutions have also stressed that countries need to “ensure that any measure taken to combat terrorism comply with all their obligations under international law ... in particular international human rights, refugee, and humanitarian law” (Security Council Resolution 1456 (2003))—something that China’s proposed legislation clearly does not do.

The draft counterterrorism law states that “counterterrorism work shall be conducted in accordance with the law” and that “human rights shall be respected and guaranteed” (art. 6). But the 106-article draft makes clear the government’s intent to establish a counterterrorism structure with enormous discretionary powers, define terrorism and terrorist activities so broadly as to easily include peaceful dissent or criticism of the government or the Communist Party’s ethnic and religious policies, and set up a total digital surveillance architecture subject to no legal or legislative control. (See below: China’s Draft Counterterrorism Law: Key Areas of Concern)

In recent years China has experienced a number of deadly and apparently politically motivated attacks directed against the general population. Since 2009 several hundred people have died in Xinjiang in attacks on police stations, train stations, and public markets. Some attacks have also taken place outside of Xinjiang. On March 1, 2014, in one of the most serious incident to date, 8 knife-wielding men and women attacked a crowd at Kunming train station, in Yunnan province, killing 29 and injuring 143, according to **official accounts**.

At the same time, the Chinese government has long manipulated the threat of terrorism to justify its crackdown on the 10 million ethnic Uyghurs in Xinjiang. Human rights violations **documented by Human Rights Watch** in recent years include broad denial of political, cultural and religious rights, torture and enforced disappearances, extensive censorship, and pervasive socio-economic discrimination.

“While terrorism poses grave threats to society, overbroad and abusive counterterrorism measures can also inflict grave harm and exacerbate conflict,” Richardson said. “Harsh measures that conflate political or religious dissent with crime discourage ordinary people from trusting or cooperating with law enforcement agencies.”

Over the past three years **hundreds of people have been killed by law enforcement personnel** in what the authorities claimed were counterterrorism operations, raising serious concerns about regular disproportionate use of force, especially since China systematically prevents independent

monitoring of the region. This situation makes it impossible to assess the veracity of general and specific claims by the Chinese government of terrorist incidents or threats.

To reduce the risk of militancy and politically motivated violence, Human Rights Watch said, the Chinese government should immediately remove curbs on the rights to freedom of expression, religion and association, strengthen the independence of the judiciary, end torture and ill-treatment of criminal suspects, and strengthen effective human rights protections.

“Targeting people for attack is never justified, but committing human rights violations is no way to stop such horrific violence,” said Richardson. “The Chinese government needs to respect rights, not build a new architecture of surveillance.”

China’s Draft Counterterrorism Law: Key Areas of Concern

Many aspects of the current draft counterterrorism law are incompatible with international human rights law and could facilitate future human rights violations. Given the lack of an independent judiciary, the pervasive character of human rights violations in China, and the criminalization of peaceful political challenges to one-party rule by the Communist Party, the draft law raises serious concerns regarding privacy, police powers, counterterrorism interventions abroad, and freedom of association and expression.

Serious Concerns Include:

1. The Definition of what Constitutes “Terrorism” is Dangerously Vague and Open-Ended

The draft law’s definition of terrorism includes “thought, speech, or behavior” that attempt to “influence national policy-making,” “subvert state power,” or “split the state” (art. 104). The first criterion is overly broad and could potentially apply to anyone advocating for policy changes. The two other criteria have been regularly used to prosecute peaceful dissenters and critics of government or Party policies, including the Nobel Peace Prize Laureate Liu Xiaobo and the Uyghur economist Ilham Tohti (sentenced respectively to **11 years** and **life imprisonment**). The definition of what constitutes “terrorism” also tautologically refers to “other terrorist activities,” potentially allowing any activity to be deemed a terrorist offense. The offenses of “advocating, inciting, or instigating” terrorism and “supporting, assisting, or facilitating” a terrorist organization or terrorists includes these same overly broad definitions.

2. Terrorism is Conflated with Religious “Extremism”

Under China’s already restrictive religion policies, the term “religious extremism” is routinely employed to characterize and often prosecute religious activities that take place outside state-controlled religious institutions, even if that activity is well within the boundaries of freedom of

religion as defined under international law. Among the broad conduct identified as “extremist” by the draft law feature: “distorting or attacking state policies, laws, and administrative regulations,” “using ethnicity or religion to ... interfere in production or management,” and “forcing minors to take part in religious activities,” as well as open-ended clauses such as “other conducts that disrupt the implementation of state policy, laws, administrative rules and regulations” (art. 24).

In Xinjiang, minors have long been prohibited by law from participating in any religious activity. Under the draft law, defying these restrictions could now be characterized as “terrorist or extremist tendencies”. Behavior deemed “extremist” is to be subject to reeducation, censorship, and punishment (art. 26).

3. The Designation of Terrorist Organizations by the State is Devoid of Due Process Protections

The draft law would establish a new counterterrorism body, the “leading organ on counterterrorism work” (*fankongbuzhuyi gongzuo lingdao jigou*) It will have the power to designate organizations and members as terrorists (arts. 68-72). Membership in a designated terrorist group is criminalized regardless of the actions or the intent of the individual members (art. 71). The draft law states that this determination can be appealed, but not in court, only to the “leading organ on counterterrorism work”—the body that will have made the initial determination (art. 72).

In the past, the Chinese government has labeled as “terrorist” organizations that openly rejected violence but were critical of government policies, such as exile groups including the **World Uyghur Congress** and the **Tibetan Youth Congress**.

4. Enforcing a System of Complete, Permanent Digital Surveillance

All telecommunication and Internet service providers would be required to provide the government with “backdoors” and a copy of the encryption systems they use, and assist with decryption (arts. 15-16, 94). Requiring companies to do so could actually undermine security because these services would be more vulnerable to hacking. All telecommunication and online service providers would be required to store user data within China’s borders (arts. 15, 93). Providers that do not comply will not be allowed to operate in China (art. 15). This information will be networked with the new national counterterrorism intelligence center (arts. 41-52).

Major transport hubs, streets, and public spaces will be outfitted with facial recognition equipment that will cross-check the information collected against a database of wanted suspects (arts. 23, 46). Such a system could easily be abused for personal or political ends, or used to track political

dissenters and others for peaceful activities protected under international human rights law. The draft law does not establish a time limit for keeping the data, nor does it define which agencies and under what procedures they will be able to access it.

In the absence of any meaningful protections, and given the near complete absence of privacy statutes in China, Human Rights Watch is concerned that this architecture of surveillance will be used to suppress peaceful political dissent, target human rights and other civil society activists, and suppress particular religious or ethnic groups deemed suspect by the law enforcement agencies.

5. The Authority and Powers of the New Body in Charge of Coordinating Counterterrorism Work are Vague

The new “leading organ on counterterrorism work” is vested with considerable powers to carry out “all work on counterterrorism nationwide.” However, the draft law gives no details about the source of its legal authority and the authority to which it will report, its operations, and its staffing. The draft law merely states that this structure will have an “office” in charge of “day to day work,” corresponding bodies at the local (provincial, municipal and prefectural) level (art. 10), and that a “national counterterrorism intelligence center” will be established to centralize information between the “relevant departments” (art. 41).

6. The Draft Law Would Expand Coercive and Surveillance Powers of Law Enforcement Agencies

Law enforcement agencies would be allowed to impose a wide range of restrictive measures on terrorism suspects, such as prohibitions against leaving particular locations, communicating with specific people, or engaging in “large-scale social activities” or “business activities” (art. 52). These measures are not subjected to court authorization or a time limitation, and could easily be abused or applied arbitrarily, without legal recourse.

7. The Draft Law Would Allow Counterterrorism Missions Beyond China’s Borders

The People’s Liberation Army, the People’s Armed Police, the Public Security and the State security would be able to carry out “counterterrorism missions” abroad with the approval of the country concerned (art. 76.) The open-ended definition of “terrorism” used in the draft law would facilitate abusive acts in violation of China’s extra-territorial obligations to respect international human rights law.

8. The Draft Law Targets Nongovernmental Organizations

The draft law includes a specific section on nongovernmental organizations (NGOs) receiving foreign funding, reflecting the suspicion with which the Chinese government regards civil society

groups. The law would require banks and related government departments to monitor the funding flow of foreign NGOs that operate in China, as well as that of foundations and other non-profit agencies. It also would require these organizations to report their financial situations and funding sources to the government agencies that sponsor them.

Such requirements are already part of the regulatory framework for NGOs and so are unnecessarily included in the counterterrorism law. The Chinese authorities have often used alleged tax or financial infractions to justify politically motivated arrests and prosecutions of civil society figures, such as the legal activist **Xu Zhiyong** in 2009 and the filmmaker **Shen Yongping** in 2014. The inclusion of such measures in a counterterrorism law means that NGOs would now be subject to investigation for much more serious offenses and face potentially much harsher penalties.

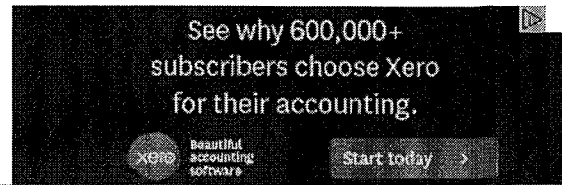
Region / Country Asia, China and Tibet

Topic Terrorism / Counterterrorism, Press Freedom, Free Speech, Internet Freedom

More Reading

Exhibit BB

THE DIPLOMAT
Read The Diplomat, Know the Asia-Pacific



Beijing Strikes Back in US-China Tech Wars

Foreign tech firms will either have to comply with intrusive surveillance requirements or risk being substituted by Chinese alternatives.

By **Ankit Panda**
March 06, 2015



Image Credit: China Internet concept via Shutterstock.com

China's new draft anti-terror legislation has sent waves across the U.S. tech community. If there is a brewing tech war between U.S. and China over government surveillance backdoors and a preference for indigenous software, China's new draft terror law makes it clear that Beijing is happy to give the United States a taste of its own medicine. The law has already drawn considerable criticism from international human rights groups, including Amnesty International and Human Rights Watch for its purported attempts to legitimize wanton human rights violations in the name of counter-terrorism. Additionally, China has opted to implement its own definition of terrorism, placing "any thought, speech, or activity that, by means of violence, sabotage, or threat, aims to generate social panic, influence national policy-making, create ethnic hatred, subvert state power, or split the state" under the umbrella of the overused T-word.

The problematic human rights issues aside, the draft anti-terror law will have important implications for foreign tech firms within China. According to *Reuters'* reporting on the draft anti-terror law, counter-terrorism precautions by the Chinese government would essentially require foreign firms to "hand over encryption keys and install security 'backdoors'" into their software. Additionally, these firms would have to store critical data — certainly data on Chinese citizens and residents — on Chinese soil. The onerous implications of this law could have lead to an immediate freeze to the activities of several Western tech companies in China, the world's second largest economy and a booming emerging market for new technologies.

On the surface, the most troublesome implication of this law is that in order to comply with this law, Western firms, including non-technical ventures such as financial institutions and manufacturers, will be forced to give up a great deal of security. In essence, corporate secrets, financial data — all critical data — would be insecure and available for access by Chinese regulators. The new law would also prohibit the use of secure virtual private networks (VPNs)

to get around these requirements.

The U.S. diplomatic response to Beijing's new draft law is perhaps best captured in the fact that a whopping *four* cabinet members in the Obama administration, including Secretary of State John Kerry and U.S. Trade Representative Michael Froman, wrote the Chinese government expressing "serious concern." China, for its part, seemed unfazed by U.S. concerns. Foreign Ministry spokesperson Hua Chunying told the press that she hoped the United States would view the new anti-terror precautions in "in a calm and objective way." Indeed, following Edward Snowden's revelations regarding the extent of the United States' surveillance of private firms both within and outside the United States, Beijing likely views U.S. concerns as hypocritical. One U.S. industry source told *Reuters* that the new law was "the equivalent of the Patriot Act on really, really strong steroids."

The draft anti-terror law fits into broader plans by the Chinese government to evacuate "key sectors" of foreign software. Chinese President Xi Jinping called for the government to use more domestic technology as early as a year ago, at the first meeting of the Internet security and informatization group. In Xi's view, for China to become a more secure cyber power, it needs to know how its critical software was developed and minimize opportunities for foreign cyber infiltration. This means by 2020, China will look to entirely wean itself off Microsoft operating systems and IBM software solutions to homegrown alternatives (China released its "people's OS" in August 2014).

The U.S. will likely not back down from its current position on this new law. The Obama administration, in its diplomacy with China, has ensured that it sends positive signals to the United States' vibrant tech industry. For example, last year, when the U.S. Department of Justice indicted five PLA officers for cyber espionage, one explanation proffered for the indictment was that it would let U.S. companies know that the government would impose costs on Beijing for the alleged theft of private intellectual property.

Froman has already said that the new law "[isn't] about security," alleging instead that it is "about protectionism and favoring Chinese companies." The United States will have a tough time convincing Beijing of the same. Given the confluence of cybersecurity and anti-terrorism issues in this law — two incredibly sensitive topics for China — negotiations will not be easy, if they are possible at all.

You have read 3 of your **5 free articles** this month.

Subscribe to Diplomat All-Access

Enjoy **full access** to the website *and* get an automatic subscription to our magazine with a *Diplomat All-Access* subscription.

Subscribe Now

Exhibit CC



EDITION: U.S.

SIGN IN | REGISTER

Search Reuters

[HOME](#) [BUSINESS](#) [MARKETS](#) [WORLD](#) [POLITICS](#) [TECH](#) [OPINION](#) [BREAKINGVIEWS](#) [MONEY](#) [LIFE](#) [PICTURES](#) [VIDEO](#)

Technology | Mon Mar 2, 2015 6:07pm EST

Related: WORLD, TECH, CHINA

Exclusive: Obama sharply criticizes China's plans for new technology rules

WASHINGTON | BY JEFF MASON

Missing Plug-in

President Barack Obama on Monday sharply criticized China's plans for new rules on U.S. tech companies, urging Beijing to change the policy if it wants to do business with the United States and saying he had raised it with President Xi Jinping.

In an interview with Reuters, Obama said he was concerned about Beijing's plans for a far-reaching counterterrorism law that would require technology firms to hand over encryption keys, the passcodes that help protect data, and install security "backdoors" in their systems to give Chinese authorities surveillance access.

"This is something that I've raised directly with President Xi," Obama said. "We have made it very clear to them that this is something they are going to have to change if they are to do business with the United States."

The Chinese government sees the rules as crucial to protect state and business secrets. Western companies say they reinforce increasingly onerous terms of doing business in the world's second-largest economy and heighten mistrust over cybersecurity between Washington and Beijing.

A Chinese parliamentary body read a second draft of the country's first anti-terrorism law last week and is expected to adopt the legislation in the coming weeks or months.

The initial draft, published by the National People's Congress late last year, requires companies to also keep servers and user data within China, supply law enforcement authorities with communications records and censor terrorism-related Internet content.

The laws "would essentially force all foreign companies, including U.S. companies, to turn

over to the Chinese government mechanisms where they can snoop and keep track of all the users of those services," Obama said.

"As you might imagine tech companies are not going to be willing to do that," he said.

The scope of the rules reaches far beyond a recently adopted set of financial industry regulations that pushed Chinese banks to purchase from domestic technology vendors.

The implications for Silicon Valley companies, ranging from Microsoft Corp (MSFT.O) to Apple Inc (AAPL.O), have set the stage for yet another confrontation over cybersecurity and technology policy, a major irritant in U.S.-China relations.

Obama said the rules could also backfire on China.

"Those kinds of restrictive practices I think would ironically hurt the Chinese economy over the long term because I don't think there is any U.S. or European firm, any international firm, that could credibly get away with that wholesale turning over of data, personal data, over to a government," he said.

A U.S. official told Reuters last week that the Obama administration has conveyed its concerns about the anti-terrorism draft law to China.

REGULATORY PRESSURE

Although the counterterrorism provisions would apply to both domestic and foreign technologies, officials in Washington and Western business lobbies argue the law, combined with the new banking rules and a slew of anti-trust investigations, amount to unfair regulatory pressure targeting foreign companies.

To be sure, Western governments, including in the United States and Britain, have for years requested tech firms to disclose encryption methods, with varying degrees of success.

Officials including FBI director James Comey and National Security Agency (NSA) director Mike Rogers publicly warned Internet companies including Apple and Google late last year against using encryption that law enforcement cannot break.

Beijing has argued the need to quickly ratchet up its cybersecurity measures in the wake of former NSA contractor Edward Snowden's revelations of sophisticated U.S. spying techniques.

China is drafting the anti-terrorism law at a time when Chinese leaders say the country faces a serious threat from religious extremists and separatists. Hundreds of people have been killed over the past two years in the far-western region of Xinjiang in unrest the government has blamed on Islamists who want to establish a separate state called East Turkestan.

(Writing by Jason Szep; Editing by Grant McCool)



IN PHOTOS: SUPER TUESDAY



Our latest photos from the crucial primary date. [Slideshow »](#)

[Campaigning with the family](#)

[The endorsement game](#)



Now available for iPhone



Ever thought you could win the presidency? [Download Now »](#)

TRENDING ON REUTERS

- U.N. imposes harsh new sanctions on North Korea drafted by U.S., China **1**
- Bin Laden called for Americans to rise up over climate change **2**
- Supreme Court hears high-stakes Texas abortion case **3**
- How the Republican elite turned a blind eye to the rise and rise of Donald Trump **4**
- Huge quake strikes off Indonesia but tsunami warnings canceled **5**

Exhibit DD

Hard National Security Choices

LAWFARE

  SUPPORT

Wednesday, March 2, 2016

-  [TOPICS](#)
 - [HOME](#)
 - [REVIEWS](#) 
 - [FOREIGN POLICY ESSAY](#)
 - [SPECIAL FEATURES](#) 
 - 
-
- [OMPHALOS](#)
 - [PODCASTS](#) 
 - [AEGIS](#)
 - [MORE](#) 

CHINA

Apple in China, Part I: What Does Beijing Actually Ask of Technology Companies?

By [Samm Sacks](#) Monday, February 22, 2016, 7:30 AM

Apple’s challenge to a court order requiring the company assists the US government in unlocking the iPhone of one of the San Bernardino shooters has led to a [discussion](#) about what exactly Apple provides to the *Chinese* government. [Some reports](#) have speculated that while Apple defies the US government, it has no problem acquiescing to Beijing’s security demands—including the possibility that the company already may be providing Beijing exactly the sort of “backdoors” it will not give the FBI. Others allege that Apple’s stand in the US is necessary in order for the company to adopt a similar hard line in China.



Samm Sacks is a Senior Analyst at Eurasia Group focusing on political risk in China. She specializes in Chinese technology and cybersecurity policy. Previously, she was an analyst at Booz Allen Hamilton and Defense Group Inc. She has also worked at the Council on Foreign Relations and was a Fulbright Scholar in Beijing. She has an MA from Yale University in International Relations and BA from Brown University in Chinese Literature.

[MORE ARTICLES](#) 

RELATED ARTICLES

[Water Wars: Missile-Deployment Controversy Splashes on, as PRC Foreign](#)

Only Apple and the Chinese government know for sure the nature of their relationship, and what Apple is willing and obligated to provide.

But in the absence of that information, a close reading of China’s applicable laws and regulations is the best guide to understanding the obligations that foreign technology companies take on in exchange for access to China’s market. These laws and regulations leave plenty of room for interpretation and negotiation by individual companies.

To lend some needed factual basis to the ongoing debate, the following is a primer for understanding the legal and regulatory environment companies like Apple face in China.

Understanding Beijing’s Approach to ICT and Cybersecurity Policy

Currently, the Chinese government—not unlike US authorities—is in the process of developing a legal and regulatory regime to catch up with the growth of new technologies, particularly in the internet and information communications technology (ICT) sectors. The senior political ranks in Beijing recognize that the government’s ability to control, censor, and supervise the technology and the information it transmits has fallen behind and must now catch up. Essentially, the technology has gotten ahead of the government’s ability to manage it.

Minister Visits Washington

Zack Bluestone Fri, Feb 26, 2016,
2:24 PM

Water Wars: China Makes Waves with Missile Deployment After Uneventful U.S.-ASEAN Summit

Lawfare Staff Fri, Feb 19, 2016,
2:58 PM

Water Wars: Calm Before Potential ASEAN-Summit Storm

Lawfare Staff Fri, Feb 12, 2016,
11:02 AM

Water Wars: U.S. Navy Back for FON in the South China Sea

Lawfare Staff Fri, Feb 5, 2016,
10:25 AM

Water Wars: American Angling Ahead of ASEAN Summit

Lawfare Staff Fri, Jan 29, 2016,
10:25 AM

SUPPORT
LAWFARE

Top leaders, including President Xi Jinping, are pushing for “protecting national sovereignty in cyberspace” (维护国家网络空间主权). The phrase appears repeatedly in policy directives and senior official statements dating back to at least 2010. It is intended to capture that the Chinese Communist Party maintains ultimate control over the internet and the ICT business environment in China in a way as to create, over time, national borders in cyberspace or even fragmentation of the global internet as the Party seeks to preserve domestic stability.

There are three primary relevant laws and an additional host of industry-specific regulations related to network and information security. These rules should not be read in isolation, but instead as mutually reinforcing elements of Beijing’s collective effort to increase security controls in cyberspace. Together these laws reflect Beijing’s increasingly hardline approach to ICT policy as the government seeks to increase control over networks, data, and information transmission.

Key Laws and Regulations

Below are highlights from these laws and regulations.

National Security Law

The National People's Congress (NPC) passed the National Security Law in July 2015. The National Security Law operates as the legal framework to bolster control across all sectors of the economy under the banner of a sweeping definition of security that includes the economy, financial system, indigenous technology innovation, and social stability. The language is deliberately broad and will serve as basis for more detailed regulations, which are currently pending.

In the section on technology and information security, the familiar “protecting national sovereignty in cyberspace” language appears. And although the concept is not new, here Beijing elevates its importance by enshrining it in national law.

The National Security Law will likely lay the groundwork for more formalized reviews of inbound foreign investment, somewhat akin to the Committee on Foreign Investment in the United States (CFIUS), an interagency body in the US government. In the Chinese system, there are currently only national security review bodies dedicated to examining foreign investments in China's four free trade zones (FTZs) in Fujian, Tianjin, Guangdong, and Shanghai. However, under the new law, these review bodies are likely to extend to foreign investments nationwide, and they will take a far more expansive view of national security than counterparts like CFIUS do in within the US. It is

possible that, over the coming years, foreign tech firms will be required to undergo multiple separate security reviews at different levels in the bureaucracy—the Chinese government is now also setting up a cybersecurity review body and yet-to-be disclosed industry-specific approvals and certifications, including one on data localization.

Counterterrorism Law

The NPC passed a Counterterrorism (CT) Law in December 2015. There are three important points to note about this law. The first is that the government made key changes between the draft and the final version and that those changes created more ambiguity in terms of what companies must provide to the government. The original language in the draft law required telecom operators and internet service providers (ISPs) to install “backdoors” in their products and report encryption keys to the government. The final version of the law, however, only says these types of companies must extend technical interfaces, decryption, and other technical assistance and support to anti-terror authorities.

It would thus appear that the new language waters down the original requirements. But the new language is also vague, and the government has not yet issued implementation details. Typically, the government first issues a law of

broad principles and then clarifies the scope in a series of implementation decrees. Foreign technology firms are currently in the process of trying to predict and understand how the government will implement and enforce these broad new measures. Moreover, there are separate pending revisions to the 1999 Commercial Encryption Regulations. It would not be surprising if the government folds the encryption requirements that were removed from the CT law into this regulation.

The second point is that the encryption clause in the counterterrorism law only applies to telecom operators and internet services providers; Apple does not fall into either of these categories. And finally, note that the government has removed entirely a provision from the original draft that would have required telecom operators and ISPs to store all data and equipment in China.

These changes represent a modest victory for foreign ICT companies. Most importantly, the changes reflect that Beijing was at least somewhat responsive to pressure from US industry lobbies and the US government.

But that's hardly the end of the story in China. Data localization remains a top priority for Beijing; the fact that it has disappeared from this particular law does not mean Beijing has backed down on the issue. To the contrary, the government has rolled out data localization requirements in other—less high-profile—industry-specific regulations it has released

since the passage of the CT law. For example, last week the Ministry of Industry and Information Technology (MIIT) and the State Administration of Press Publication Radio Film and Television (SAPPRFT) unveiled new measures that require localization of server and storage equipment for online publishing and take effect March 10. Additionally, the draft cybersecurity law (see below) still contains data and equipment localization requirements.

Cybersecurity Law

In July 2015, shortly following the passage of the National Security Law, the NPC released the full text of the draft Cybersecurity Law. Here the government is working to create a legal basis for expanding its authority to preserve “cyberspace sovereignty” by outlining obligations of ICT companies and users.

The law faces two more rounds of review, and therefore, the content is still subject to change. Similar to the national security law, the language of the cybersecurity law is vague and broad. And as with other laws, the government will clarify the scope in follow-on decrees after the law is passed. But there is likely to be some space for discretion in how authorities implement the regulations; this may provide maneuverability for US tech firms, but could as

easily justify stringent interpretation by officials who offer little transparency in their decision-making processes.

In terms of substance, there are two relevant elements in the draft law's content. First, the draft emphasizes that companies will be required to undergo security inspections and reviews in order to be in compliance with the government's rules, but the text offers no details on what these will entail. And second, the draft law mandates that information infrastructure operators store user data within the territory of mainland China. Companies may apply for exceptions to this rule, but only after undergoing a still-unspecified additional audit and certification process.

In terms of political leadership, the law identifies the Cyberspace Administration of China as the top body charged with shaping and implementing cybersecurity policy. This is significant for two reasons—both of which I'll explore in depth in later posts. But in general, this body is the functional office of the Central Leading Group for Network Security and Information chaired directly by President Xi Jinping himself. This means that now cybersecurity policy is coming from the highest levels in the Chinese bureaucracy, whereas previously it had been fragmented with turf wars among lower-level players. Furthermore, the CAC is notoriously inaccessible to foreign companies in China—which means

that efforts to engage with government stakeholders when it comes to the regulatory landscape will be extremely difficult.

“Secure and Controllable” Regulations

The Chinese government has also set out new security requirements in industry-specific regulations. The phrase “secure and controllable” (安全可控) is sometimes also referred to as “secure and reliable” (安全可靠) or “indigenous and controllable” (自主可控). Since August alone, the phrase has appeared in separate pending rules for ICT used in insurance, medical devices, and the Internet Plus sectors (i.e. smart technology, cloud computing, mobile technology, and e-commerce).

Because this standard has no single definition, the government and Chinese industry have broad discretionary authority to launch intrusive security audits or reject foreign suppliers altogether as not secure. And while many of these regulations are still pending, Chinese government and industry is already moving forward with informal implementation of the standard, by asking foreign vendors to certify that they are “secure and controllable.”

There are numerous interpretations of the phrase, but one thing is clear: the government is linking localization with security, which means

that Chinese companies have a competitive advantage when it comes to meeting these new security standards. This puts foreign technology companies in a weaker negotiating position, and adds to pressure that they cooperate with local partners, rather than attempting to go it alone in the market.

Common Practices and Informal Pressures

Beyond the new and pending laws and regulations, foreign firms already face pressure to submit source code, undergo security audits, and localize data and equipment. These procedures are costly and expose foreign tech companies to a host of security, regulatory, and IP risks in order to be in the market.

Foreign tech firms have been providing at least partial source code to the Chinese government for years. For example, Microsoft provided Windows source code to the Chinese government in the 1990s. And it remains the common practice today. Providing source code is not necessarily the same as providing so-called “backdoor” access to device contents, but it does have significant security implications. And understanding the ongoing provision of such information is necessary to meaningfully evaluate the consequences of other requirements.

Similarly, security audits are also a regular part of operating in the China market. In practice, a security audit could range from something as benign as sitting down for a series of meetings with government officials—perhaps from the Ministry of Public Security—and answering questions about security features, data storage, or management techniques to something far more invasive. And as a consequence of the pending laws and regulations, these security reviews are likely to become increasingly intensive.

These requirements and practices underscore the fact that foreign enterprise in China is never as simple as it seems. And the obligations on foreign companies are still quite in flux.

Topics: China, Cybersecurity, Encryption

Tags: Apple

Exhibit EE

QUARTZ

What Chinese slowdown? Apple's sales double in China on iPhone growth

Alice Truong | October 27, 2015

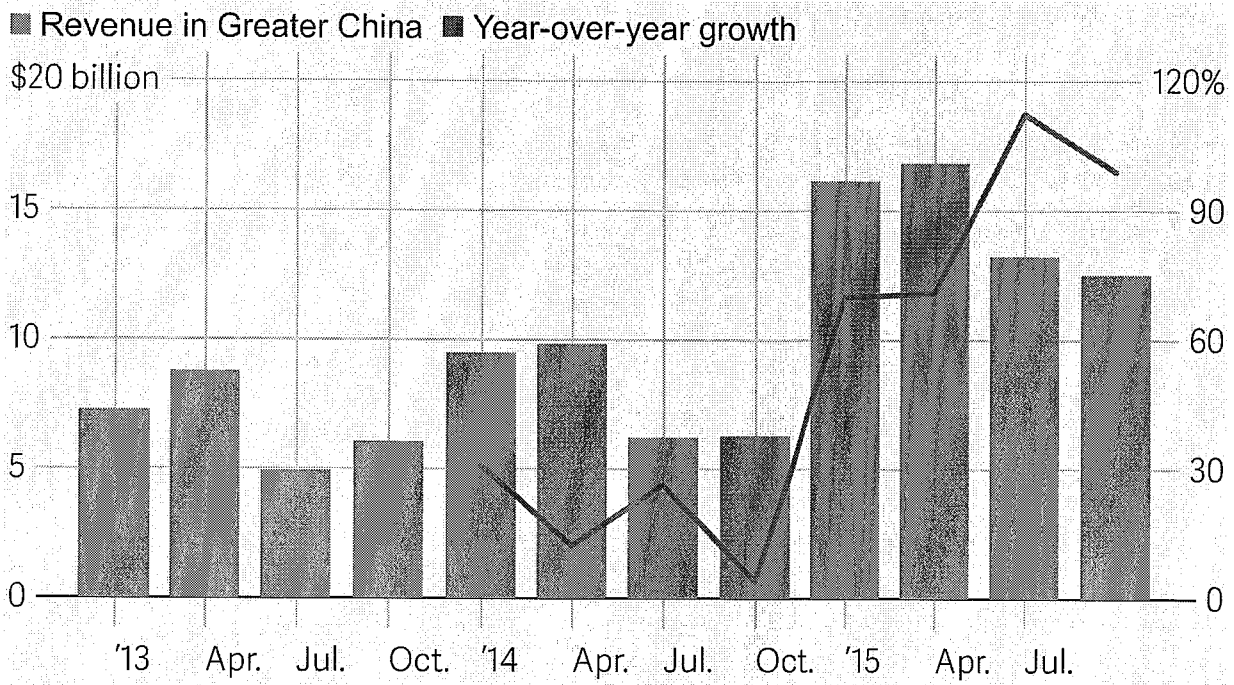


📷 Got mine. (AP Photo/Andy Wong)

Apple certainly hasn't noticed a dent in its China business. The company reported 99% year-over-year revenue growth in the fourth quarter in China. CEO Tim Cook told investors today (Oct. 27) that he anticipates the Greater China region will become "Apple's top market in the world," though he didn't say when. Already Greater China, which includes Taiwan and Hong Kong, accounts for 24% of Apple's

total revenue.

Apple's sales in China



ATLAS | Data: Apple

Share

“Frankly, if I were to shut off my web and shut off the TV and just look at how many customers are coming in our stores regardless of whether they’re buying, how many people are coming online, and in addition looking at our sales trends,” Cook said, “I wouldn’t know there was any economic issue at all in China.” China’s long-anticipated economic slowdown hit the economy this year, and recently pulled quarterly GDP growth below 7% for the first time since 2009.

But, according to Cook, Apple’s retail stores in Greater China “are among the busiest in the world.” The company just opened its 25th outpost in the region, with plans for a total of 40 by mid 2016.

Sales in Greater China were driven largely by the iPhone, with revenue for the device climbing 87% year-over-year in the region and 120% in the mainland—where the iPhone 6 was the best-selling smartphone last quarter—compared with 22% growth globally. Half of the consumers in China who bought an iPhone 6 or 6 Plus

were buying their first Apple smartphone, Cook said. The company also saw a 127% rise in App Store revenue, driven by more than 1 million developers in China building for iOS.

Cook, not surprisingly, is optimistic about the continued growth of China's middle class. Apple, he said, will continue "investing for the decades ahead" in China.

NEW INQUIRIES

The gendered way we've learned to ask questions is terrible for both men and women

Elizabeth Weingarten | 5 hours ago



📷 Men and women in the dating world often feel they face a communication breakdown. (AP Photo/Thibault Camus)

"Thank god you picked up," I whispered to my best friend. I was huddled in the

Exhibit FF

350 Fifth Avenue, 34th Floor
New York, NY 10118-3299
Tel: 212-290-4700
Fax: 212-736-1300; 917-591-3452



HRW.org

ASIA DIVISION

Brad Adams, *Executive Director*
Kanae Doi, *Japan Director*
Meenakshi Ganguly, *South Asia Director*
Phelim Kine, *Deputy Director*
Elaine Pearson, *Australia Director*
Sophie Richardson, *China Director*
Phil Robertson, *Deputy Director*
John Sifton, *Advocacy Director*
Mickey Spiegel, *Senior Advisor*
Heather Barr, *Senior Researcher*
Andreas Harsono, *Senior Researcher*
David Mathieson, *Senior Researcher*
Sunai Phasuk, *Senior Researcher*
Tejshree Thapa, *Senior Researcher*
Jayshree Bajoria, *Researcher*
Carlos H. Conde, *Researcher*
Saroop Ijaz, *Researcher*
Maya Wang, *Researcher*
Riyo Yoshioka, *Senior Program Officer*
Ahmad Shuja, *Research Associate*
Storm Tiv, *Senior Associate*
Shayna Bauchner, *Associate*
Georgia Bright, *Associate*
Daniel Lee, *Associate*

ADVISORY COMMITTEE

David Lakhdhir, *Chair*
Orville Schell, *Vice-Chair*
Maureen Aung-Thwin
Edward J. Baker
Robbie Barnett
Robert L. Bernstein
Jerome Cohen
John Despres
Mallika Dutt
Kek Galabru
Merle Goldman
Jonathan Hecht
Sharon Hom
Rounaq Jahan
Ayesha Jalal
Robert James
Joanne Leedom-Ackerman
Perry Link
Kimberly Marteau Emerson
Krishen Mehta
Andrew J. Nathan
Xiao Qiang
Bruce Rabb
Balakrishnan Rajagopal
Ahmed Rashid
Victoria Riskin
James Scott
Mark Sidel
Eric Stover
Ko-Yung Tung
Francesc Vendrell
Tuong Vu

HUMAN RIGHTS WATCH

Kenneth Roth, *Executive Director*
Michele Alexander, *Deputy Executive Director, Development and Global Initiatives*
Carroll Bogert, *Deputy Executive Director, External Relations*
Iain Levine, *Deputy Executive Director, Program*
Chuck Lustig, *Deputy Executive Director, Operations*

Dinah PoKempner, *General Counsel*
James Ross, *Legal & Policy Director*
Hassan Elmasry, *Co-Chair*
Joel Motley, *Co-Chair*

August 4, 2015

Li Shishi
Chairman
Legislative Affairs Commission
No. 1, Qianmenxi Street
Xicheng District, Beijing 100805
The People's Republic of China
Email: icc@npc.gov.cn

Submission by Human Rights Watch to the National People's Congress Standing Committee on the draft Cybersecurity Law

Human Rights Watch is an international nongovernmental organization that monitors and reports on human rights in about 90 countries around the world. We welcome the opportunity to provide comments on the draft Cybersecurity Law ("the draft law"), which was published by the National People's Congress Standing Committee Legislative Affairs Commission on its website on July 6, 2015. Human Rights Watch advocates compliance with international human rights law globally, including the rights to privacy, freedom of expression, and access to information that are at the heart of the draft law.

Human Rights Watch has examined the draft law in detail and urges the Chinese government to substantially revise it to scrap provisions that require Internet companies to practice censorship, register users' real names, localize data, and aid government surveillance.

The Chinese government's pervasive use of censorship and broad surveillance is well-documented. The draft law, which further institutionalizes and strengthens these practices, will limit healthy debates in society as well as exchanges important for technological, scientific, and other social advancements.

Human Rights Watch's specific concerns about the draft law include:

1. Requirements for companies to censor and restrict online anonymity

The draft law requires Internet companies to demand that users provide their real name and personal information (art. 20). It also requires companies to provide unspecified “necessary assistance” to police when investigating crimes and for “state security reasons” (art. 23), and to censor undefined “prohibited” messages, stop their spread, cease providing services to the offenders, and report the incidents to the authorities (arts. 40-43). Companies can be fined, their licenses cancelled, and businesses closed if they fail to comply with these requirements (arts. 53 and 57). Article 50 also allows local governments to suspend or restrict local Internet services upon higher level approval when it is necessary to protect “state security.”

The rights to freedom of expression and to privacy are protected both by the Chinese Constitution and the International Covenant on Civil and Political Rights, which China has signed but not yet ratified. The right to privacy and the right to freedom of expression entail a corollary right to communicate anonymously. Allowing people to speak anonymously has long been recognized as worthy of protection in order to encourage communication that might otherwise invite reprisal or stigmatization, such as anonymous tips for journalists or blowing the whistle on fraud and improprieties in the workplace or government. The ability to seek, impart, or receive information anonymously online creates a “zone of privacy to protect opinion and belief” and other rights. Although governments have an obligation to investigate and prosecute crimes, they should not impose blanket prohibitions on anonymity, as they are neither necessary nor proportionate; this view is forcefully articulated in the May 2015 report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye. That same report also urges governments to refrain from making identification of users (that is, real-name registration) a condition for access to online services.

Chinese laws, including the draft law, do not clearly define “state security,” a fact that was recently criticized by the UN High Commissioner for Human Rights. As a result, those laws allow the term to be arbitrarily or broadly misapplied by the state security apparatus in a wide range of circumstances, including crushing peaceful protests and censoring messages critical of the government.

2. Requirements for “all critical information infrastructure operators” to localize data

Article 31 of the draft law mandates that “all critical information infrastructure operators” store data in China, though it allows for exceptions upon passing a security review. Article 25 broadly defines “critical information infrastructure” as, among other things, “basic information networks such as public communications ... services” as well as “networks

and systems managed or owned by Internet service providers with many users,” and thus could include most Internet companies.

This requirement would allow the government greater access to and control over user data. In the absence of effective safeguards against the government’s abuse of such access, there is great potential for user privacy to be violated. Such a requirement should be removed from the draft law completely.

3. Requirements for companies to monitor undefined “network security incidents”

The draft law also requires operators to adopt technological measures for monitoring network security incidents and retaining network logs (art. 17(3)). Government departments are also required to establish such measures and implement response plans in the case of network security incidents (arts. 44-50). However, the draft does not define “network security incidents,” though Article 65(2) refers “network security” to the prevention of “attacks, invasion, disturbance, undermining and unlawful use of networks ... unexpected accidents.” The wide range of circumstances which could be construed as “network security incidents” raises concerns about broad, increased surveillance of online activity.

4. Lack of effective mechanisms to protect privacy

Although the draft law also requires network operators and other companies to protect personal data and notify users of potential security vulnerabilities (arts. 18 and 34-37), and stipulates punishments for such privacy breaches (art. 54), the provisions are vague. It is unclear how users’ privacy can be protected given the broad powers the draft law gives to the government and companies to restrict it, and given the lack of effective mechanisms to challenge privacy violations in China, including when such violations are committed by security agencies in the name of protecting “state security.”

Thank you for your attention to this important matter. We look forward to hearing from you.

Sincerely,



Sophie Richardson
China Director
Human Rights Watch

Exhibit GG

English.news.cn



Search

Advanced Search

Missing Plug

Editions

Services | Database | Markets | Weather | Site Index | RSS | Feedback

Global Edition | China | World | Business | Culture & Edu | Sports | Entertainment | Science & Technology | Health | Travel | Odd News | In-Depth

Most Searched: •SDR •AIB •Refugee •Paris attacks •Syria

Provisions of China's counterterrorism bill inspired by foreign laws: official

English.news.cn 2015-12-27 19:19:35



BEIJING, Dec. 27 (Xinhua) -- China has studied U.S. and European Union laws in drafting its own counterterrorism bill which requires tech firms to assist security authorities to prevent and investigate terrorism, an legislative official said here Sunday.

At a press conference held at the end of a week-long session of China's top legislature, Li Shouwei of the National People's Congress (NPC) Standing Committee legislative affairs commission, admitted that a number of countries and enterprises had voiced concerns about certain provisions in the law.

He pointed to Article 18 of the new law, which requires telecom operators and internet service providers to provide technical support and assistance, including decryption, to police and national security authorities in prevention and investigation of terrorist activities.

Li said the rule accorded with the actual work need of fighting terrorism and was basically the same as what other major countries in the world do.

"The clause reflects lessons China has learnt from other countries and is a result of wide solicitation of public opinion," he added.

"(It) will not affect companies' normal business nor install backdoors to infringe intellectual property rights, or ... citizens freedom of speech on the internet and their religious freedom," Li said.

Editor: Tian Shaohui



Share

Related News

- China adopts first counter-terrorism law
- Commentary: U.S. shows insincerity in fighting terrorism by smearing China's anti-terrorism law
- China slams U.S. double standards on terrorism



Photos >>



Chinese FM meets with secretary-general of OAS in Beijing



Ex-Zimbabwe VP launches new party to challenge Mugabe in 2018 polls



Alibaba's Internet lender extends 45 bln yuan in loans in 8 months



Children attend first day of classes in Panama



Original signed images of David Beckham displayed in London



Zhang Xinyi promotes new TV drama in Beijing



NASA begins work to bring back supersonic passenger travel



Herbal supplements linked with at least six organ transplants in Australia

Follow Xinhua



Facebook



Twitter



YouTube



Sina Weibo

Photos >>



In pics: Icicles at Hukou waterfall on Yellow River



Chinese lantern show held in California



In pics: Winter fishing in NE China



Yoga players practice in sunset glow in China's Hubei



Visitors have fun at "Ice Carnival" in N. China



Snow blankets Beijing

Video >>



U.S.-backed alliance captures key dam in Syria



Russia to begin delivery of S-300 to Iran



- China's 1st anti-domestic violence law takes effect
- Beijing eases rules for permanent residence permits
- What is Super Tuesday?
- Tourism development must include protection
- Recalling the Ancient Silk Road

Back to Top

Special Reports >>



2015 World Internet Conference

Yearender 2015

Exhibit HH

United Nations

A/HRC/23/40



General Assembly

Distr.: General
17 April 2013

Original: English

Human Rights Council

Twenty-third session

Agenda item 3

**Promotion and protection of all human rights, civil,
political, economic, social and cultural rights,
including the right to development**

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*

Summary

The present report, submitted in accordance with Human Rights Council resolution 16/4, analyses the implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression. While considering the impact of significant technological advances in communications, the report underlines the urgent need to further study new modalities of surveillance and to revise national laws regulating these practices in line with human rights standards.

* Late submission.

A/HRC/23/40

Contents

	<i>Paragraphs</i>	<i>Page</i>
I. Introduction	1-6	3
II. Activities of the Special Rapporteur	7-10	4
III. The evolution of technology of surveillance	11-18	4
IV. International human rights framework	19-32	6
A. Interrelations between the rights to privacy to freedom of opinion and expression	24-27	7
B. Permissible limitations to privacy and freedom of expression	28-29	8
C. Recent considerations by international mechanisms for the protection of human rights	30-32	9
V. Modalities of communications surveillance	33-49	10
A. Targeted communications surveillance.....	34-37	10
B. Mass communications surveillance	38-40	11
C. Access to communications data	41-43	11
D. Internet filtering and censorship	44-46	12
E. Restrictions on anonymity	47-49	13
VI. Concerns on national legal standards	50-71	13
A. Lack of judicial oversight	54-57	14
B. National security exceptions	58-60	15
C. Unregulated access to communications data	61	16
D. Extra-legal surveillance	62-63	16
E. Extra-territorial application of surveillance laws	64	17
F. Mandatory data retention	65-67	17
G. Identity disclosure laws	68-70	18
H. Restrictions on encryption and key disclosure laws	71	19
VII. The roles and responsibilities of the private sector	72-77	19
VIII. Conclusions and recommendations	78-99	20
A. Updating and strengthening laws and legal standards	81-87	21
B. Facilitating private, secure and anonymous communications.....	88-90	22
C. Increasing public access to information, understanding and awareness of threats to privacy	91-94	22
D. Regulating the commercialization of surveillance technology	95-97	22
E. Furthering the assessment of relevant international human rights obligations	98-99	23

I. Introduction

1. The present report analyses the implications of States' surveillance of communications for the exercise of the human rights to privacy and to freedom of opinion and expression. While considering the impact of significant technological advances in communications, the report underlines the urgent need to further study new modalities of surveillance and to revise national laws regulating these practices in line with human rights standards.

2. Innovations in technology have increased the possibilities for communication and protections of free expression and opinion, enabling anonymity, rapid information-sharing and cross-cultural dialogues. Technological changes have concurrently increased opportunities for State surveillance and interventions into individuals' private communications.

3. Concerns about national security and criminal activity may justify the exceptional use of communications surveillance technologies. However, national laws regulating what would constitute the necessary, legitimate and proportional State involvement in communications surveillance are often inadequate or non-existent. Inadequate national legal frameworks create a fertile ground for arbitrary and unlawful infringements of the right to privacy in communications and, consequently, also threaten the protection of the right to freedom of opinion and expression.

4. In previous reports (A/HRC/17/27 and A/66/290), the Special Rapporteur has analysed the unprecedented impact of the Internet on expanding the possibilities of individuals to exercise their right to freedom of opinion and expression. He expressed concerns at the multiple measures taken by States to prevent or restrict the flow of information online, and highlighted the inadequate protection of the right to privacy in the Internet.

5. Building on his previous analysis, the aim of this report is to identify the risks that the new means and modalities of communications surveillance pose to human rights, including the right to privacy and the freedom of opinion and expression.

6. The following terms are used in this report to describe the most common modalities of surveillance of communications:

(a) Communications surveillance: the monitoring, interception, collection, preservation and retention of information that has been communicated, relayed or generated over communications networks;

(b) Communications data: information about an individual's communications (e-mails, phone calls and text messages sent and received, social networking messages and posts), identity, network accounts, addresses, websites visited, books and other materials read, watched or listened to, searches conducted, resources used, interactions (origins and destinations of communications, people interacted with, friends, family, acquaintances), and times and locations of an individual, including proximity to others);

(c) Internet filtering: automated or manual monitoring of Internet content (including websites, blogs and online media sources, as well as e-mail) to restrict or suppress particular text, images, websites, networks, protocols, services or activities.

A/HRC/23/40

II. Activities of the Special Rapporteur

7. During the reporting period, the Special Rapporteur participated in multiple international and national events related to the issues he addressed in his previous reports such as freedom of expression in the Internet, prevention of hate speech, and the protection of journalists. He paid particular attention to national initiatives promoting the protection of journalists; in this regard, he participated in meetings on initiatives developed in Brazil, Colombia, Honduras and Mexico. He also participated in the "United Nations Inter-Agency Meeting on the Safety of Journalists and the Issues of Impunity", held in November 2012 in Vienna.

8. His last report to the United Nations General Assembly focused on prevention of hate speech and incitement to hatred.¹ The same topic was addressed in a side event to the General Assembly jointly organized by the Special Rapporteur and the Special Adviser on the Prevention of Genocide in February 2013. In the same month, he further addressed these issues in the launch of the "Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence" in Geneva and in the Fifth United Nations Alliance of Civilizations Global Forum in Vienna.

9. The Special Rapporteur undertook a mission to Honduras from 7 to 14 August 2012. His main findings and recommendations on this visit can be found in the addendum to this report (A/HRC/20/40/Add.1). He was invited by the Indonesian Government to visit the country in January 2013. Regrettably, the Government requested the visit to be postponed and new dates for the visit are yet to be confirmed.

10. For the preparation of this report, the Special Rapporteur revised relevant studies and consulted with experts on matters related to the surveillance of communications. In December 2012, he participated in the Workshop on Electronic Surveillance and Human Rights organized by the Electronic Frontier Foundation. In February 2013, he organized an expert consultation for the preparation of this report which took place in parallel to the activities of the "World Summit on the Information Society+10 Meeting" held at the United Nations Educational, Scientific and Cultural Organization (UNESCO), Paris, where he also participated in the opening plenary panel.

III. The evolution of technology of surveillance

11. Innovations in technology have facilitated increased possibilities for communication and freedom of expression, enabling anonymity, rapid information sharing, and cross-cultural dialogues. At the same time, changes in technologies have also provided new opportunities for State surveillance and intervention into individuals' private lives.

12. From the inception of the first form of remote communications, States have sought to intercept and monitor individuals' private communications to serve law enforcement and national security interests. Through communications, the most personal and intimate information, including about an individual's or group's past or future actions, can be revealed. Communications represent a valuable source of evidence upon which the State can draw to prevent or prosecute serious crimes or forestall potential national security emergencies.

¹ A/67/357.

13. Innovations in technology throughout the twentieth century changed the nature and implications of communication surveillance. The means by, and frequency with which people are able to communicate expanded significantly. The transition from fixed-line telephone systems to mobile telecommunication and the declining costs of communications services resulted in dramatic growth in telephone usage. The advent of the Internet saw the birth of a number of new tools and applications to communicate at no cost, or at very affordable rates. These advancements have enabled greater connectivity, facilitated the global flow of information and ideas, and increased the opportunities for economic growth and societal change.

14. As information and communication technologies evolved, so did the means by which States sought to monitor private communications. With increased use of telephones came the use of wiretapping, which consists of placing a tap on a telephone wire to listen to private phone conversations. With the replacement of analogue telephone networks with fibre optics and digital switches in the 1990s, States redesigned the networking technology to include interception capabilities (“backdoors”) to permit State surveillance, rendering modern telephone networks remotely accessible and controllable.

15. The dynamic nature of technology has not only changed how surveillance can be carried out, but also “what” can be monitored. In enabling the creation of various opportunities for communication and information-sharing, the Internet has also facilitated the development of large amounts of transactional data by and about individuals. This information, known as communications data or metadata, includes personal information on individuals, their location and online activities, and logs and related information about the e-mails and messages they send or receive. Communications data are storable, accessible and searchable, and their disclosure to and use by State authorities are largely unregulated. Analysis of this data can be both highly revelatory and invasive, particularly when data is combined and aggregated. As such, States are increasingly drawing on communications data to support law enforcement or national security investigations. States are also compelling the preservation and retention of communication data to enable them to conduct historical surveillance.

16. Changes in technology have been paralleled by changes in attitudes towards communications surveillance. When the practice of official wiretapping first commenced in the United States of America, it was conducted on a restricted basis, and was only reluctantly sanctioned by the courts.² It was viewed as such a serious threat to the right to privacy that its use had to be restricted to detecting and prosecuting the most serious crimes. Over time, however, States have expanded their powers to conduct surveillance, lowering the threshold and increasing the justifications for such surveillance.

17. In many countries, existing legislation and practices have not been reviewed and updated to address the threats and challenges of communications surveillance in the digital age. Traditional notions of access to written correspondence, for example, have been imported into laws permitting access to personal computers and other information and communications technologies, without consideration of the expanded uses of such devices

² In the first judicial validation of wiretapping, Justice Brandeis of the United States Supreme Court wrote a scathing dissent that noted that wiretapping was a “subtler and more far-reaching means of invading privacy” that could not be justified under the Constitution. In a chillingly accurate forecast, the eminent jurist predicted: “Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrence of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions.” *Olmstead v. United States*, 277 U.S. 438 (1928).

and the implications for individuals' rights. At the same time, the absence of laws to regulate global communications surveillance and sharing arrangements has resulted in ad hoc practices that are beyond the supervision of any independent authority. Today, in many States, access to communications data can be conducted by a wide range of public bodies for a wide range of purposes, often without judicial authorization and independent oversight. In addition, States have sought to adopt surveillance arrangements that purport to have extra-territorial effect.

18. Human rights mechanisms have been equally slow to assess the human rights implications of the Internet and new technologies on communications surveillance and access to communications data. The consequences of expanding States' surveillance powers and practices for the rights to privacy and freedom of opinion and expression, and the interdependence of those two rights, have yet to be comprehensively considered by the Human Rights Council, special procedures mandate holders or human rights treaty bodies. This report seeks to rectify this.

IV. International human rights framework

19. The right to freedom of opinion and expression is guaranteed under articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, which affirm that everyone has the right to hold opinions without interference, and to seek, receive and impart information and ideas of all kinds through any media and regardless of frontiers. At the regional level, the right is protected by the African Charter on Human and Peoples' Rights (art. 9), the American Convention on Human Rights (art. 13); and the Convention for the Protection of Human Rights and Fundamental Freedoms (art. 10).

20. At both the international and regional levels, privacy is also unequivocally recognized as a fundamental human right. The right to privacy is enshrined by the Universal Declaration of Human Rights (art. 12), the International Covenant on Civil and Political Rights (ICCPR, art. 17), the Convention on the Rights of the Child (art. 16), and the International Convention on the Protection of All Migrant Workers and Members of Their Families (art. 14). At the regional level, the right to privacy is protected by the European Convention on Human Rights (art. 8) and the American Convention on Human Rights (art. 11).

21. Despite the widespread recognition of the obligation to protect privacy, the specific content of this right was not fully developed by international human rights protection mechanisms at the time of its inclusion in the above-mentioned human rights instruments. The lack of explicit articulation of the content of this right has contributed to difficulties in its application and enforcement.³ As the right to privacy is a qualified right, its interpretation raises challenges with respect to what constitutes the private sphere and in establishing notions of what constitutes public interest. The rapid and monumental changes to communications and information technologies experienced in recent decades have also irreversibly affected our understandings of the boundaries between private and public spheres.

22. Privacy can be defined as the presumption that individuals should have an area of autonomous development, interaction and liberty, a "private sphere" with or without interaction with others, free from State intervention and from excessive unsolicited

³ UNESCO, *Global Survey on Internet Privacy and Freedom of Expression*, 2012, p. 51.

intervention by other uninvited individuals.⁴ The right to privacy is also the ability of individuals to determine who holds information about them and how is that information used.

23. In order for individuals to exercise their right to privacy in communications, they must be able to ensure that these remain private, secure and, if they choose, anonymous. Privacy of communications infers that individuals are able to exchange information and ideas in a space that is beyond the reach of other members of society, the private sector, and ultimately the State itself. Security of communications means that individuals should be able to verify that their communications are received only by their intended recipients, without interference or alteration, and that the communications they receive are equally free from intrusion. Anonymity of communications is one of the most important advances enabled by the Internet, and allows individuals to express themselves freely without fear of retribution or condemnation.

A. Interrelations between the rights to privacy to freedom of opinion and expression

24. The right to privacy is often understood as an essential requirement for the realization of the right to freedom of expression. Undue interference with individuals' privacy can both directly and indirectly limit the free development and exchange of ideas. Restrictions of anonymity in communication, for example, have an evident chilling effect on victims of all forms of violence and abuse, who may be reluctant to report for fear of double victimization. In this regard, article 17 of ICCPR refers directly to the protection from interference with "correspondence", a term that should be interpreted to encompass all forms of communication, both online and offline.⁵ As the Special Rapporteur noted in a previous report,⁶ the right to private correspondence gives rise to a comprehensive obligation of the State to ensure that e-mails and other forms of online communication are actually delivered to the desired recipient without the interference or inspection by State organs or by third parties.⁷

25. The Human Rights Committee analysed the content of the right to privacy (art. 17) in its General Comment No. 16 (1988), according to which article 17 aims to protect individuals from any unlawful and arbitrary interferences with their privacy, family, home, or correspondence, and national legal frameworks must provide for the protection of this right. This provision imposes specific obligations relating to the protection of privacy in communications, underlining that "correspondence should be delivered to the addressee without interception and without being opened or otherwise read. "Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations, should be prohibited."⁸ The General Comment also indicates that "the gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law."⁹ At the time this General Comment was

⁴ Lord Lester and D. Pannick (eds.). *Human Rights Law and Practice*. London, Butterworth, 2004, para. 4.82.

⁵ ICCPR commentary, p.401.

⁶ A/HRC/17/23.

⁷ ICCPR commentary, p.401.

⁸ Centre for Civil and Political Rights (CCPR) General Comment No. 16. (General Comments), p.8.

⁹ *Ibid.*, p.10.

A/HRC/23/40

adopted, the impact of advances in information and communications technologies on the right to privacy was barely understood.

26. In its General Comment No. 34 (2011) on the right to freedom of expression, the Human Rights Committee indicated that States parties should take account of the extent to which developments in information and communication technologies have substantially changed communication practices. The Committee also called on States parties to take all necessary steps to foster the independence of these new media. The General Comment also analyses the relationship between the protection of privacy and freedom of expression, and recommends that States parties respect that element of the right of freedom of expression that embraces the limited journalistic privilege not to disclose information sources.¹⁰

27. Tensions also exist between the right to privacy and the right to freedom of expression, for example, when information considered to be private is disseminated through the media. In this sense, article 19 (3) provides for restrictions on freedom of expression and information to protect the rights of others. However, as it happens for all permissible limitations to the right to freedom of expression (see below), the principle of proportionality must be strictly observed, since there is otherwise danger that freedom of expression would be undermined. Particularly in the political arena, not every attack on the good reputation of politicians must be permitted, since freedom of expression and information would otherwise be stripped of their crucial importance for the process of forming political opinions,¹¹ advocating for transparency and combating corruption. The international jurisprudence at regional level indicates that in situations of conflict between privacy and freedom of expression, reference should be made to the overall public interest on the matters reported.¹²

B. Permissible limitations to privacy and freedom of expression

28. The framework of article 17 of the ICCPR enables necessary, legitimate and proportionate restrictions to the right to privacy by means of permissible limitations. In contrast with the provisions of article 19, paragraph 3, which spell out elements of a test for permissible limitations,¹³ the formulation of article 17 does not contain a limitation clause. Despite these differences in wording, it is understood that article 17 of the Covenant should also be interpreted as containing elements of a permissible limitations test already described in other General Comments of the Human Rights Committee.¹⁴

29. In this regard, the Special Rapporteur takes the position that the right to privacy should be subject to the same permissible limitations test as the right to freedom of movement, as elucidated in General Comment 27.¹⁵ The test as expressed in the comment includes, inter alia, the following elements:

- (a) Any restrictions must be provided by the law (paras. 11-12);
- (b) The essence of a human right is not subject to restrictions (para. 13);

¹⁰ CCPR General Comment No. 34.

¹¹ Nowak, Manfred, *United Nations Covenant on Civil and Political Rights: CCPR Commentary* (1993), p.462

¹² UNESCO, *Global Survey on Internet Privacy and Freedom of Expression*, 2012, pp. 53 and 99.

¹³ Lists of permissible limitations are also included in art. 12, (3), on the right to liberty of movement and freedom to choose his residence; art. 18, (3), on the right to freedom of thought, conscience and religion; art. 21, on the right of peaceful assembly; and art. 22, (2), on the right to freedom of association.

¹⁴ *Ibid.*

¹⁵ See also CCPR General Comment No. 34.

- (c) Restrictions must be necessary in a democratic society (para. 11);
- (d) Any discretion exercised when implementing the restrictions must not be unfettered (para. 13);
- (e) For a restriction to be permissible, it is not enough that it serves one of the enumerated legitimate aims. It must be necessary for reaching the legitimate aim (para. 14);
- (f) Restrictive measures must conform to the principle of proportionality, they must be appropriate to achieve their protective function, they must be the least intrusive instrument amongst those which might achieve the desired result, and they must be proportionate to the interest to be protected (paras. 14-15).

C. Recent considerations by international mechanisms for the protection of human rights

30. In previous reports, the Special Rapporteur has assessed the impact of the Internet on the realization of the right to freedom of opinion and expression (A/HRC/17/27 and A/66/290). He noted that, while Internet users can enjoy relative anonymity on the Internet, States and private actors also have access to new technologies to monitor and collect information about individuals' communications and activities. Such technologies have the potential to violate the right to privacy, thereby undermining people's confidence and security on the Internet and impeding the free flow of information and ideas online. The Special Rapporteur urged States to adopt effective privacy and data protection laws in accordance with human rights standards, and to adopt all appropriate measures to ensure that individuals can express themselves anonymously online.¹⁶

31. Other Special Procedures mandate holders considered the issue of interferences with the right to privacy. The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism studied developments in surveillance practices and technologies that have adversely affected the right to privacy using the justification of combating terrorism.¹⁷ The Special Rapporteur underscored that these measures have not only led to violations of the right to privacy, but have also had an impact on due process rights and the rights to freedom of movement, freedom of association and freedom of expression. He urged Governments to articulate in detail how their surveillance policies uphold the principles of proportionality and necessity, in accordance with international human rights standards, and what measures have been taken to protect against abuse. The Special Rapporteur also called for the adoption of comprehensive data protection and privacy laws and the establishment of strong independent oversight bodies mandated to review the use of intrusive surveillance techniques and the processing of personal information. He further called for research and development resources to be devoted to privacy-enhancing technologies.

32. Other human rights protection mechanisms have also recently paid attention to the impact of the surveillance of communications on the protection of the rights to privacy and freedom of expression. The Human Rights Committee voiced concerns, for example, at allegations of State monitoring the use of the Internet and blocking access to some websites¹⁸ and recommended the review of legislation providing the executive with wide powers of surveillance in respect of electronic communications.¹⁹ The Universal Periodic

¹⁶ A/HRC/17/27, p.22.

¹⁷ A/HRC/13/37.

¹⁸ CCPR/C/IRN/CO/3.

¹⁹ CCPR/C/SWE/CO/6.

A/HRC/23/40

Review has also included recommendations to ensure, for example, that legislation relating to the Internet and other new communication technologies respects international human rights obligations.²⁰

V. Modalities of communications surveillance

33. Modern surveillance technologies and arrangements that enable States to intrude into an individual's private life threaten to blur the divide between the private and the public spheres. They facilitate invasive and arbitrary monitoring of individuals, who may not be able to even know they have been subjected to such surveillance, let alone challenge it. Technological advancements mean that the State's effectiveness in conducting surveillance is no longer limited by scale or duration. Declining costs of technology and data storage have eradicated financial or practical disincentives to conducting surveillance. As such, the State now has a greater capability to conduct simultaneous, invasive, targeted and broad-scale surveillance than ever before.

A. Targeted communications surveillance

34. States have access to a number of different techniques and technologies to conduct communications surveillance of a targeted individual's private communications. Real-time interception capabilities allow States to listen to and record the phone calls of any individual using a fixed line or mobile telephone, through the use of interception capabilities for State surveillance that all communications networks are required to build into their systems.²¹ An individual's location can be ascertained, and their text messages read and recorded. By placing a tap on an Internet cable relating to a certain location or person, State authorities can also monitor an individual's online activity, including the websites he or she visits.

35. Access to the stored content of an individual's e-mails and messages, in addition to other related communications data, can be obtained through Internet companies and service providers. The initiative of the European standards-setting authority, the European Telecommunications Standards Institute, to compel cloud providers²² to build "lawful interception capabilities" into cloud technology to enable State authorities to have direct access to content stored by these providers, including e-mails, messages and voicemails, raises concerns.²³

36. States can track the movements of specific mobile phones, identify all individuals with a mobile phone within a designated area, and intercept calls and text messages, through various methods. Some States use off-the-air mobile monitoring devices called International Mobile Subscriber Identity (IMSI) catchers, which can be installed in a location temporarily (such as at a protest or march) or permanently (such as at an airport or other border crossings). These catchers imitate a mobile phone tower by sending and

²⁰ A/HRC/14/10.

²¹ See, for example, the United States Communications Assistance for Law Enforcement Act 1994 (United States); Telecommunications Act 1997, Part 15 (Australia); Regulation of Investigatory Powers Act 2000, ss12-14 (United Kingdom); Telecommunications (Interception Capability) Act 2004.

²² A cloud provider offers services of networked online storage of data.

²³ ETSI DTR 101 567 VO.0.5 (2012-14), Draft Technical Report: Lawful Interception (LI); Cloud/Virtual Services (CLI).

responding to mobile phone signals in order to extract the unique subscriber identification module (SIM) card number of all mobile phones within a certain territory.

37. States are also increasingly acquiring software that can be used to infiltrate an individual's computer, mobile phone or other digital device.²⁴ Offensive intrusion software, including so-called "Trojans" (also known as spyware or malware), can be used to turn on the microphone or camera of a device, to track the activity conducted on the device, and to access, alter or delete any information stored on the device. Such software enables a State to have complete control of the device infiltrated, and is virtually undetectable.

B. Mass communications surveillance

38. Costs and logistical hurdles to conduct surveillance on a mass scale continue to decline rapidly, as technologies allowing for broad interception, monitoring and analysis of communications proliferate. Today, some States have the capability to track and record Internet and telephone communications on a national scale. By placing taps on the fibre-optic cables, through which the majority of digital communication information flows, and applying word, voice and speech recognition, States can achieve almost complete control of tele- and online communications. Such systems were reportedly adopted, for example, by the Egyptian and Libyan Governments in the lead-up to the Arab Spring.²⁵

39. In many States, mandatory data retention is facilitating massive collection of communications data that can later be filtered and analysed. Technologies enable the State to scan phone calls and text messages to identify the use of certain words, voices or phrases, or filter Internet activity to determine when an individual visits certain websites or accesses particular online resources. "Black boxes" can be designed to inspect the data flowing through the Internet in order to filter through and deconstruct all information about online activity. This method, called "deep-packet inspection", allows the State to go beyond gaining simple knowledge about the sites that individuals visit, and instead analyse the content of websites visited. Deep-packed inspection, for example, has been reportedly employed by States confronted with recent popular uprisings in the Middle East and North Africa region.²⁶

40. Another tool used regularly by States today is social media monitoring. States have the capacity physically to monitor activities on social networking sites, blogs and media outlets to map connections and relationships, opinions and associations, and even locations. States can also apply highly sophisticated data mining technologies to publicly available information or to communications data provided by third party service providers. At a more basic level, States have also acquired technical means to obtain usernames and passwords from social networking sites such as Facebook.²⁷

C. Access to communications data

41. In addition to intercepting and tracking the content of individuals' communications, States may also seek access to communications data held by third party service providers and Internet companies. As the private sector collects progressively larger amounts of

²⁴ Toby Mendel, Andrew Puddephatt, Ben Wagner, Dixi Hawtin, and Natalia Torres, *Global Survey on Internet Privacy and Freedom of Expression, UNESCO Series on Internet Freedom* (2012), p. 41.

²⁵ European Parliament, Directorate-General for External Policies, Policy Department, *After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy* (2012), pp. 9-10.

²⁶ Mendel *et al.*, *op. cit.*, p. 43.

²⁷ European Parliament, *op. cit.*, p. 6.

A/HRC/23/40

varied data that reveal sensitive information about peoples' daily lives, and individuals and businesses choose to store the content of their communications, such as voicemails, e-mails and documents, with third party service providers, access to communications data is an increasingly valuable surveillance technique employed by States.

42. The communications data collected by third party service providers, including large Internet companies, can be used by the State to compose an extensive profile of concerned individuals. When accessed and analysed, even seemingly innocuous transactional records about communications can collectively create a profile of individual's private life, including medical conditions, political and religious viewpoints and/or affiliation, interactions and interests, disclosing as much detail as, or even greater detail than would be discernible from the content of communications alone.²⁸ By combining information about relationships, location, identity and activity, States are able to track the movement of individuals and their activities across a range of different areas, from where they travel to where they study, what they read or whom they interact with.

43. Instances of access to communications data by States are growing rapidly. In the three years that Google has been reporting the numbers of requests for communications data it receives, such requests have almost doubled, from 12,539 in the last six months of 2009, to 21,389 in the last six months of 2012.²⁹ In the United Kingdom, where law enforcement authorities are empowered to self-authorize their own requests for communications information, approximately 500,000 such requests were reported every year.³⁰ In the Republic of Korea, a country of nearly 50 million people, there are approximately 37 million requests for communications data reported every year.³¹

D. Internet filtering and censorship

44. Advances in technology have not only facilitated interception of and access to communications in specific cases, but have also enabled States to conduct widespread, even nationwide, filtering of online activity. In many countries, Internet filtering is conducted under the guise of maintaining social harmony or eradicating hate speech, but is in fact used to eradicate dissent, criticism or activism.

45. Filtering technologies mentioned above also facilitate the monitoring of web activity in order to enable the State to detect forbidden images, words, site addresses or other content, and censor or alter it. States can use such technologies to detect the use of specific words and phrases, in order to censor or regulate their use, or identify the individuals using them. In countries with high levels of Internet penetration, Internet filtering reportedly enables the censorship of website content and communications and facilitates the surveillance of human rights defenders and activists.³²

46. In addition to technologies that facilitate filtering and censorship, many States are conducting manual Internet filtering, by creating online police forces and inspectors in order to physically monitor the content of websites, social networks, blogs and other forms

²⁸ Alberto Escudero-Pascual and Gus Hosein, "Questioning lawful access to traffic data", *Communications of the ACM*, Volume 47 Issue 3, March 2004, pp. 77-82.

²⁹ See <http://www.google.com/transparencyreport/userdatarequests/>.

³⁰ See <http://www.intelligencecommissioners.com/docs/0496.pdf>.

³¹ Money Today, 23 October, 2012, citing the disclosure made by the Korean Communication Commission for the Annual National Audit of 2013 to Assemblywoman Yoo Seung-Hui, <http://www.mt.co.kr/view/mtview.php?type=1&no=2012102309430241764&outlink=1>.

³² European Parliament, Directorate-General for External Policies, Policy Department, After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy (2012), p. 12.

of media. In some States, “cyber police forces” are tasked with inspecting and controlling the Internet, searching websites and critical nodes within websites (particularly online discussion forums) with a view to block or shut down websites whenever they contain content the Government disapproves of, including or criticism of the country’s leadership. The burden of such policing is transferred to private intermediaries, such as search engines and social network platforms, through laws that widen liability for proscribed content from the original speaker to all intermediaries.

E. Restrictions on anonymity

47. One of the most important advances facilitated by the advent of the Internet was the ability to anonymously access and impart information, and to communicate securely without having to be identified. Initially, this was possible given that there was no “identity layer” to the Internet; originally, it was not possible to know who was behind a specific communication, e-mail address, or even a given computer. However, in the name of security and law enforcement, gradually States have been eradicating the opportunities for anonymous communication. In many States, individuals must identify themselves at cybercafés and have their transactions on public computers recorded. Increasingly, identification and registration are also required when buying a SIM card or mobile telephone device, for visiting certain major websites, or for making comments on media sites or blogs.

48. Restrictions on anonymity facilitate State communications surveillance by simplifying the identification of individuals accessing or disseminating prohibited content, making such individuals more vulnerable to other forms of State surveillance.

49. In this sense, restrictions on anonymity have a chilling effect, dissuading the free expression of information and ideas. They can also result in individuals’ de facto exclusion from vital social spheres, undermining their rights to expression and information, and exacerbating social inequalities. Furthermore, restrictions on anonymity allow for the collection and compilation of large amounts of data by the private sector, placing a significant burden and responsibility on corporate actors to protect the privacy and security of such data.

VI. Concerns on national legal standards

50. Generally, legislation has not kept pace with the changes in technology. In most States, legal standards are either non-existent or inadequate to deal with the modern communications surveillance environment. As a result, States are increasingly seeking to justify the use of new technologies within the ambits of old legal frameworks, without recognizing that the expanded capabilities they now possess go far beyond what such frameworks envisaged. In many countries, this means that vague and broadly conceived legal provisions are being invoked to legitimize and sanction the use of seriously intrusive techniques. Without explicit laws authorizing such technologies and techniques, and defining the scope of their use, individuals are not able to foresee – or even know about – their application. At the same time, laws are being adopted to broaden the breadth of national security exceptions, providing for the legitimization of intrusive surveillance techniques without oversight or independent review.

51. Inadequate legal standards increase the risk of individuals being exposed to violation of their human rights, including the right to privacy and the right to freedom of expression. They also have an adverse impact on certain groups of individuals – for example, members of certain political parties, trade unionists or national, ethnic and linguistic minorities – who

A/HRC/23/40

may be more vulnerable to State communications surveillance. Without strong legal protections in place, journalists, human rights defenders and political activists risk being subjected to arbitrary surveillance activities.

52. Surveillance of human rights defenders in many countries has been well documented. On these occasions, human rights defenders and political activists report having their phone calls and e-mails monitored, and their movements tracked. Journalists are also particularly vulnerable to becoming targets of communications surveillance because of their reliance on online communication. In order to receive and pursue information from confidential sources, including whistleblowers, journalists must be able to rely on the privacy, security and anonymity of their communications. An environment where surveillance is widespread, and unlimited by due process or judicial oversight, cannot sustain the presumption of protection of sources. Even a narrow, non-transparent, undocumented, executive use of surveillance may have a chilling effect without careful and public documentation of its use, and known checks and balances to prevent its misuse.

53. The following subsections list common concerns regarding laws that allow State surveillance of communications surveillance in circumstances that threaten the rights to freedom of expression and privacy.

A. Lack of judicial oversight

54. Whereas traditionally communications surveillance was required to be authorized by the judiciary, increasingly this requirement is being weakened or removed. In some countries, interception of communications can be authorized by a governmental minister, their delegate, or a committee. In the United Kingdom, for example, interception of communications is authorized by the Secretary of State,³³ in Zimbabwe, interception of communications is authorized by the Minister for Transport and Communication.³⁴ Progressively, communications surveillance can also be authorized on a broad and indiscriminate basis, without the need for law enforcement authorities to establish the factual basis for the surveillance on a case-by-case basis.

55. Many States have dispensed with the need for law enforcement agencies to return to the court for ongoing supervision after an interception order is issued. Under the Kenyan Prevention of Terrorism Act 2012, for example, interception of communications can be conducted over an indefinite period of time, without any requirement that law enforcement agencies report back to a court or seek an extension. Some States impose time limits on the execution of interception orders but enable law enforcement authorities to renew such orders repeatedly and indefinitely.

56. Even when judicial authorization is required by law, often it is de facto an arbitrary approval of law enforcement requests. This is particularly the case where the threshold required to be established by law enforcement is low. For example, the Ugandan Regulation of Interception of Communications Act 2010 only requires law enforcement authorities to demonstrate that "reasonable" grounds exist to allow the interception to take place. In such instances, the burden of proof to establish the necessity for surveillance is extremely low, given the potential for surveillance to result in investigation, discrimination or violations of human rights. In other countries, a complex array of laws authorizes access to and surveillance of communications under a range of different circumstances. In Indonesia, for example, the Psychotropic Law, Narcotics Law, Electronic Information and Transaction

³³ Section 5, Regulation of Investigatory Powers Act 2000.

³⁴ Section 5, Interception of Communications Act 2006.

Law, Telecommunications Law and the Corruption Law all contain communications surveillance components. In the United Kingdom, over 200 agencies, police forces and prison authorities are authorized to acquire communications data under the Regulation of Investigatory Powers Act, 2000. As a result, it is difficult for individuals to foresee when and by which State agency they might be subjected to surveillance.

57. In many States, communication service providers are being compelled to modify their infrastructure to enable direct surveillance, eliminating the opportunity for judicial oversight. For example, in 2012 the Colombian Ministries of Justice, and Information and Communication Technologies, issued a decree that required telecommunication service providers to put in place infrastructure allowing direct access to communications by judicial police, without an order from the Attorney General.³⁵ The above-mentioned Uganda's Regulation of Interception of Communications Act 2010 (s3) provides for the establishment of a monitoring centre and mandates that telecommunications providers ensure that intercepted communications are transmitted to the monitoring centre (s8(1)(f)). The Government of India is proposing to install a Centralized Monitoring System that will route all communications to the central Government, allowing security agencies to bypass interaction with the service provider.³⁶ Such arrangements take communications surveillance out of the realm of judicial authorization and allow unregulated, secret surveillance, eliminating any transparency or accountability on the part of the State.

B. National security exceptions

58. Vague and unspecified notions of "national security" have become an acceptable justification for the interception of and access to communications in many countries. In India, for example, the Information Technology Act of 2008 allows interception of communications in the interest of, *inter alia*, "the sovereignty, integrity, or defense of India, friendly relations with foreign States, public order and the investigation of any offence" (section 69).

59. In many cases, national intelligence agencies also enjoy blanket exceptions to the requirement for judicial authorization. For example, in the United States, the Foreign Intelligence Surveillance Act empowers the National Security Agency to intercept communications without judicial authorization where one party to the communication is located outside the United States, and one participant is reasonably believed to be a member of a State-designated terrorist organization. German law allows warrantless automated wiretaps of domestic and international communications by the State's intelligence services for the purposes of protecting the free democratic order, existence or security of the State.³⁷ In Sweden, the Law on Signals Intelligence in Defense Operations authorizes the Swedish intelligence agency to intercept without any warrant or court order all telephone and Internet traffic that take place within Sweden's borders. In the United Republic of Tanzania, the Intelligence and Security Service Act 1996 enables the country's intelligence services to conduct any investigations and investigate any person or body which it has reasonable cause to consider a risk or a source of risk or a threat to the State security.

60. The use of an amorphous concept of national security to justify invasive limitations on the enjoyment of human rights is of serious concern.³⁸ The concept is broadly defined

³⁵ Ministries of Justice and ICTs Decree 1704. Rooted in the Criminal Procedure Code of 2004.

³⁶ Department of Communications. Government of India. Annual Report 2011-2012 pg. 58 – <http://www.dot.gov.in/annualreport/AR%20Engsih%2011-12.pdf>.

³⁷ G-10 law.

³⁸ Counter-terrorism Human Rights Council resolutions.

A/HRC/23/40

and is thus vulnerable to manipulation by the State as a means of justifying actions that target vulnerable groups such as human rights defenders, journalists or activists. It also acts to warrant often unnecessary secrecy around investigations or law enforcement activities, undermining the principles of transparency and accountability.

C. Unregulated access to communications data

61. Access to communications data held by domestic communications service providers is often mandated by legislation or a condition upon which licences are issued. As a result, States are generally provided with *carte blanche* access to communications data with little oversight or regulation. For example, a 2012 Brazilian law on money laundering gives police the power to access registration information from Internet and communication providers without a court order.³⁹ At the international level, the provision of access to communications data is regulated by bilateral Mutual Legal Assistance Treaties. However, this cooperation also often occurs outside of the law on the basis of the voluntary compliance of the service provider or Internet company. As such, access to communications data can be obtained in many States without independent authorization and with limited oversight.

D. Extra-legal surveillance

62. A number of the surveillance capabilities listed above fall outside of existing legal frameworks, but have nevertheless been widely adopted by States. Offensive intrusion software such as Trojans, or mass interception capabilities, constitute such serious challenges to traditional notions of surveillance that they cannot be reconciled with existing laws on surveillance and access to private information. These are not just new methods for conducting surveillance; they are new forms of surveillance. From a human rights perspective, the use of such technologies is extremely disturbing. Trojans, for example, not only enable a State to access devices, but also enable them to alter – inadvertently or purposefully – the information contained therein. This threatens not only the right to privacy and procedural fairness rights with respect to the use of such evidence in legal proceedings. Mass interception technology eradicates any considerations of proportionality, enabling indiscriminate surveillance. It enables the State to copy and monitor every single act of communication in a particular country or area, without gaining authorization for each individual case of interception.

63. Governments often do not acknowledge the use of such technologies to conduct surveillance, or argue that such technologies are being legitimately employed under the ambit of existing surveillance legislation. Although it is clear that many States possess offensive intrusion software, such as Trojan technology, the legal basis for its use has not been publicly debated in any State, with the exception of Germany. In that context, the province of North Rhine-Westphalia passed legislation in 2006 authorizing the “secret access to an information technology system” (§ 5.2 no. 11, North Rhine-Westphalia Constitution Protection Act), which was understood to be technical infiltration which is effected either by installing a spy programme or taking advantage of the security loopholes of the system. The German Federal Constitutional Court quashed the law in February 2008, ruling that such measures would only be in conformity with human rights if they were

³⁹ Brazilian Federal Law 12683/2012. Article 17-B. Available at: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12683.htm.

subject to judicial authorization and review, and occurred only in situations where there might be a concrete danger to a predominantly important legal interest.⁴⁰

E. Extra-territorial application of surveillance laws

64. In response to the increased data flows across borders and the fact the majority of communications are stored with foreign third party service providers, a number of States have begun to adopt laws that purport to authorize them to conduct extra-territorial surveillance or to intercept communications in foreign jurisdictions. This raises serious concern with regard to the extra-territorial commission of human rights violations and the inability of individuals to know that they might be subject to foreign surveillance, challenge decisions with respect to foreign surveillance, or seek remedies. In South Africa, for example, the General Intelligence Laws Amendment Bill allows for surveillance of foreign communications outside of South Africa or passing through South Africa.⁴¹ In October 2012, the Dutch Ministry of Justice and Security proposed legislative amendments to the Dutch Parliament that would allow the police to break into computers and mobile phones both within the Netherlands and abroad in order to install spyware and search and destroy data.⁴² In December 2012, Pakistan's National Assembly passed the Fair Trial Act of 2012, paragraph 31 of which provides for the execution of surveillance warrants in foreign jurisdictions. Later that month, the United States renewed the Foreign Intelligence Surveillance Amendment Act of 2008 extending the Government's power to conduct surveillance of non-American persons locate outside the United States (§1881a), including any foreign individual whose communications are hosted by cloud services located in the United States (such as Google and other large Internet companies).⁴³ Also in 2012, the European Telecommunications Standards Institute created draft standards for interception of foreign cloud-based services by European Governments.⁴⁴ These developments suggest an alarming trend towards the extension of surveillance powers beyond territorial borders, increasing the risk of cooperative agreements between State law enforcement and security agencies to enable the evasion of domestic legal restrictions.

F. Mandatory data retention

65. In order to increase the storage of communications data that they are able to access, some States are adopting mandatory data retention laws requiring Internet and telecom service providers (collectively, "communications service providers") continuously to collect and preserve communications content and information about users' online activities. Such laws enable the compilation of historical records about individuals' e-mails and messages, locations, interactions with friends and family, etc.

⁴⁰ Available in German. BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1 - 67), http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html.

⁴¹ Section 1. c. General Intelligence Laws Amendment Bill. Available at: http://www.parliament.gov.za/live/commonrepository/Processed/20111201/385713_1.pdf.

⁴² See <http://www.edri.org/edri/number10.20/dutch-proposal-state-spyware>.

⁴³ See European Parliament Directorate-General for Internal Policies Policy Department C: Citizens Rights and Constitutional Affairs, *Fighting crime and protecting privacy in the cloud: study*, 2012.

⁴⁴ Draft ESTI DTR 101 567 Lawful Interception (LI) Vo.1.0 (2012 - 05); Cloud/Virtual Services (CLI). Available at: www.3gpp.org.

A/HRC/23/40

66. In delivering services to their users, communications service providers give subscribers' devices or network an Internet Protocol (IP) address⁴⁵ that changes periodically. Information about an IP address can be used to ascertain the identity and location of an individual and track their online activity. Mandatory data retention laws force communications service providers to keep records of their IP address allocations for a certain period of time, allowing the State greater ability to require communications service providers to identify an individual on the basis of who had a given IP address at a particular date and time. Some States are also now seeking to compel third party service providers to collect and retain information that they would not normally collect.

67. National data retention laws are invasive and costly, and threaten the rights to privacy and free expression. By compelling communications service providers to create large databases of information about who communicates with whom via a telephone or the Internet, the duration of the exchange, and the users' location, and to keep such information (sometimes for years), mandatory data retention laws greatly increase the scope of State surveillance, and thus the scope for infringements upon human rights. Databases of communications data become vulnerable to theft, fraud and accidental disclosure.

G. Identity disclosure laws

68. In many States, laws require the provision of identification at cybercafés. Such laws are particularly problematic in countries where personal computer ownership is low and individuals rely heavily on publicly available computers. In India, for example, the Information Technology (Guidelines for Cyber Cafes) Rules 2011 require that cybercafé owners obtain identification documents from any individual visiting the cybercafé, which records must be kept for at least one year (Rule 4(2)). The cybercafé must maintain a log-register, containing, among other information, log in time and log out time, and computer terminal identification for a minimum period of one year (Rule 5(1) & 5(2)); store and maintain backups of log records of each access or login by any user for at least one year (Rule 5(4)).

69. Individuals are now also required to use their real names online in many States, and to provide official identification in order to establish their identity. In the Republic of Korea, the Information Communications Law, adopted in 2007, required users to register their real names before accessing websites with more than 100,000 visitors per day, ostensibly in order to reduce online bullying and hate speech. The law was recently overturned by the Constitutional Court on the basis that it restricted freedom of speech and undermined democracy.⁴⁶ China recently adopted the Decision to Strengthen the Protection of Online Information, requiring Internet and telecommunications providers to collect personal information about users when they sign up for Internet access, landline, or mobile phone service. Service providers allowing users to publish online are required to be able to link screen names and real identities. These real name registration requirements allow authorities to more easily identify online commentators or tie mobile use to specific individuals, eradicating anonymous expression.⁴⁷

⁴⁵ An IP address is a unique numeric code that identifies all computers or other devices connected to the Internet.

⁴⁶ Constitutional Court Decision 2010Hun-Ma47 ("Real names" decision), 23 August 2012. An official summary of the Court's decision is available on the Court's website at http://www.ccourt.go.kr/home/bpm/sentence01_list.jsp only in Korean.

⁴⁷ "China to Strengthen Internet Information Protection" - <http://www.ebeijing.gov.cn/BeijingInformation/BeijingNewsUpdate/t1292298.htm>.

70. A further initiative preventing communications anonymity is the gradual adoption of policies that require the registration of SIM cards with a subscriber's real name or government-issued identity document. In 48 countries in Africa, laws requiring individuals to register their personal information with their network provider prior to activation of pre-paid SIM cards are reportedly facilitating the establishment of extensive databases of user information, eradicating the potential for anonymity of communications, enabling location-tracking, and simplifying communications surveillance.⁴⁸ In the absence of data protection legislation, SIM users' information can be shared with Government departments and matched with other private and public databases, enabling the State to create comprehensive profiles of individual citizens. Individuals are also at risk of being excluded from use of mobile phone services (which may enable not only communication but also access to financial services) if they are unable or unwilling to provide identification to register.

H. Restrictions on encryption and key disclosure laws

71. The security and anonymity of communications are also undermined by laws that limit the use of privacy-enhancing tools that can be used to protect communications, such as encryption. Many States have now adopted laws that mandate an individual enable decryption when so ordered. The South African Regulation of Interception of Communications and Provisions of Communication-Related Information Act of 2002 requires decryption assistance from any person who possesses the decryption key.⁴⁹ Similar laws exist in Finland (Section 4(4)(a) Coercive Measures Act 1987/450), Belgium (Art. 9, Law on computer crime of 28 November 2000), and Australia (Sections 12 and 28 Cybercrime Act 2001).

VII. The roles and responsibilities of the private sector

72. The vital developments in technology that have enabled new and dynamic forms of communication have been occurred primarily in the private sector. In this sense, many of the changes in the way we communicate, receive and impart information are based on the research and innovations of corporate actors.

73. The private sector has also played a key role in facilitating State surveillance of individuals, in a number of ways. Corporate actors have had to respond to requirements that digital networks and communications infrastructure be designed to enable intrusion by the State. Such requirements were originally adopted by States in the 1990s and are becoming compulsory for all communications services providers. Increasingly, States are adopting legislation requiring that communications service providers allow States direct access to communications data or modify infrastructure to facilitate new forms of State intrusion.

74. In developing and deploying new technologies and communications tools in specific ways, corporate actors have also voluntarily taken measures that facilitate State surveillance of communications. In its simplest manifestation, this collaboration has taken the form of decisions on how corporate actors collect and process information, which allows them to

⁴⁸ Kevin P. Donovan and Aaron K. Martin, "The Rise of African SIM Registration: Mobility, Identity, Surveillance and Resistance," Information Systems and Innovation Group Working Paper Series, no. 186, London School of Economics and Political Science (2012).

⁴⁹ Section 29. South African Regulation of Interception of Communications and Provisions of Communication - Related Information Act 2002. Available at: <http://www.dac.gov.za/acts/Regulation%20of%20Interception%20of%20Communications%20Act.pdf>.

A/HRC/23/40

become massive repositories of personal information that are then accessible to States upon demand. Corporate actors have adopted specifications that enable State access or intrusion, collect excessive and revelatory information, or restrict the application of encryption and other techniques that could limit access to information by both the companies and governments. The private sector has also often failed to deploy privacy-enhancing technologies, or has implemented them less than secure ways that do not represent the state of the art.

75. In the most serious circumstances, the private sector has been complicit in developing technologies that enable mass or invasive surveillance in contravention of existing legal standards.⁵⁰ The corporate sector has generated a global industry focused on the exchange of surveillance technologies. Such technologies are often sold to countries in which there is a serious risk that they will be used to violate human rights, particularly those of human rights defenders, journalists or other vulnerable groups. This industry is virtually unregulated as States have failed to keep pace with technological and political developments.

76. States' human rights obligations require that they not only respect and promote the rights to freedom of expression and privacy, but protect individuals from violations of human rights perpetrated by corporate actors. In addition, States should exercise adequate oversight in order to meet their international human rights obligations when they contract with, or legislate for, corporate actors where there may be an impact upon the enjoyment of human rights.⁵¹ Human rights obligations in this regard apply when corporate actors are operating abroad.⁵²

77. States must ensure that the private sector is able to carry out its functions independently in a manner that promotes individuals' human rights. At the same time, corporate actors cannot be allowed to participate in activities that infringe upon human rights, and States have a responsibility to hold companies accountable in this regard.

VIII. Conclusions and recommendations

78. **Communications techniques and technologies have evolved significantly, changing the way in which communications surveillance is conducted by States. States must therefore update their understandings and regulation of communications surveillance and modify their practices in order to ensure that individuals' human rights are respected and protected.**

79. **States cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy. Privacy and freedom of expression are interlinked and mutually dependent; an infringement upon one can be both the cause and consequence of an infringement upon the other. Without adequate legislation and legal standards to ensure the privacy, security and anonymity of communications, journalists, human rights defenders and whistleblowers, for example, cannot be assured that their communications will not be subject to States' scrutiny.**

⁵⁰ For some examples of surveillance technology designed by the private sector and utilized in Libya, Bahrain, the Syrian Arab Republic, Egypt and Tunisia, see European Parliament, Directorate-General for External Policies, Policy Department, *After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy* (2012), pp. 9-10.

⁵¹ Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, Principle 5.

⁵² Human Rights Committee, Concluding Observations, Germany, December 2012.

80. In order to meet their human rights obligations, States must ensure that the rights to freedom of expression and privacy are at the heart of their communications surveillance frameworks. To this end, the Special Rapporteur recommends the following:

A. Updating and strengthening laws and legal standards

81. Communications surveillance should be regarded as a highly intrusive act that potentially interferes with the rights to freedom of expression and privacy and threatens the foundations of a democratic society. Legislation must stipulate that State surveillance of communications must only occur under the most exceptional circumstances and exclusively under the supervision of an independent judicial authority. Safeguards must be articulated in law relating to the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorize, carry out and supervise them, and the kind of remedy provided by the national law.

82. Individuals should have a legal right to be notified that they have been subjected to communications surveillance or that their communications data has been accessed by the State. Recognizing that advance or concurrent notification might jeopardize the effectiveness of the surveillance, individuals should nevertheless be notified once surveillance has been completed and have the possibility to seek redress in respect of the use of communications surveillance measures in their aftermath.

83. Legal frameworks must ensure that communications surveillance measures:

(a) Are prescribed by law, meeting a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee their application;

(b) Are strictly and demonstrably necessary to achieve a legitimate aim; and

(c) Adhere to the principle of proportionality, and are not employed when less invasive techniques are available or have not yet been exhausted.

84. States should criminalize illegal surveillance by public or private actors. Such laws must not be used to target whistleblowers or other individuals seeking to expose human rights violations, nor should they hamper the legitimate oversight of government action by citizens.

85. The provision of communications data by the private sector to States should be sufficiently regulated to ensure that individuals' human rights are prioritized at all times. Access to communications data held by domestic corporate actors should only be sought in circumstances where other available less invasive techniques have been exhausted.

86. The provision of communications data to the State should be monitored by an independent authority, such as a court or oversight mechanism. At the international level, States should enact Mutual Legal Assistance Treaties to regulate access to communications data held by foreign corporate actors.

87. Surveillance techniques and practices that are employed outside of the rule of law must be brought under legislative control. Their extra-legal usage undermines basic principles of democracy and is likely to have harmful political and social effects.

A/HRC/23/40

B. Facilitating private, secure and anonymous communications

88. States should refrain from compelling the identification of users as a precondition for access to communications, including online services, cybercafés or mobile telephony.

89. Individuals should be free to use whatever technology they choose to secure their communications. States should not interfere with the use of encryption technologies, nor compel the provision of encryption keys.

90. States should not retain or require the retention of particular information purely for surveillance purposes.

C. Increasing public access to information, understanding and awareness of threats to privacy

91. States should be completely transparent about the use and scope of communications surveillance techniques and powers. They should publish, at minimum, aggregate information on the number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation and purpose.

92. States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature and application of the laws permitting communications surveillance. States should enable service providers to publish the procedures they apply when dealing with State communications surveillance, adhere to those procedures, and publish records of State communications surveillance.

93. States should establish independent oversight mechanisms capable to ensure transparency and accountability of State surveillance of communications.

94. States should raise public awareness on the uses of new communication technologies in order to support individuals in properly assessing, managing, mitigating and making informed decisions on communications-related risks.

D. Regulating the commercialization of surveillance technology

95. States should ensure that communications data collected by corporate actors in the provision of communications services meets the highest standards of data protection.

96. States must refrain from forcing the private sector to implement measures compromising the privacy, security and anonymity of communications services, including requiring the construction of interception capabilities for State surveillance purposes or prohibiting the use of encryption.

97. States must take measures to prevent the commercialization of surveillance technologies, paying particular attention to research, development, trade, export and use of these technologies considering their ability to facilitate systematic human rights violations.

E. Furthering the assessment of relevant international human rights obligations

98. There is a significant need to advance international understanding on the protection of the right to privacy in light of technological advancements. The Human Rights Committee should consider issuing a new General Comment on the right to privacy, to replace General Comment No. 16 (1988).

99. Human rights mechanisms should further assess the obligations of private actors developing and supplying surveillance technologies.

Exhibit II

United Nations

A/HRC/13/37



General Assembly

Distr.: General
28 December 2009

Original: English

Human Rights Council

Thirteenth session

Agenda item 3

Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin

Summary

The Special Rapporteur, in chapter I of the present report, lists his key activities from 1 August to 15 December 2009. The main report, contained in chapter II, highlights several concerns of the Special Rapporteur regarding the protection of the right to privacy in the fight against terrorism. The importance of the right to privacy and data protection is highlighted in section A.

Article 17 of the International Covenant on Civil and Political Rights is flexible enough to enable necessary, legitimate and proportionate restrictions to the right to privacy. The Special Rapporteur argues, in section B, that article 17 should be interpreted as containing elements of a permissible limitations test. In this context, he calls upon States to justify why a particular aim is legitimate justification for restrictions upon article 17, and upon the Human Rights Committee to adopt a new general comment on article 17.

The Special Rapporteur highlights the erosion of the right to privacy in the fight against terrorism in section C. This erosion takes place through the use of surveillance powers and new technologies, which are used without adequate legal safeguards. States have endangered the protection of the right to privacy by not extending pre-existing safeguards in their cooperation with third countries and private actors. These measures have not only led to violations of the right to privacy, but also have an impact on due process rights and the freedom of movement — especially at borders — and can have a chilling effect on the freedom of association and the freedom of expression.

Without a rigorous set of legal safeguards and a means to measure the necessity, proportionality and reasonableness of the interference, States have no guidance on minimizing the risks to privacy generated by their new policies. The Special Rapporteur has identified, in section D, some of the legal safeguards that have emerged through policymaking, jurisprudence, policy reviews and good practice from around the world.

A/HRC/13/37

The concluding section makes recommendations to various key actors (domestic legislative assemblies, domestic executive powers and the United Nations) in order to improve the protection of the right to privacy in the fight against terrorism.

Contents

	<i>Paragraphs</i>	<i>Page</i>
I. Introduction	1-2	4
II. Activities of the Special Rapporteur	3-10	4
III. The right to privacy	11-57	5
A. The right to privacy as enshrined in constitutions and international human rights treaties	11-13	5
B. Permissible limitations to the right to privacy	14-19	6
C. Erosion of the right to privacy by counter-terrorism policies	20-47	9
D. Best practices	48-57	17
IV. Conclusions and recommendations	58-74	20
A. Conclusions	58-59	20
B. Recommendations	60-74	21

A/HRC/13/37

I. Introduction

1. This report is submitted to the Human Rights Council by the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, pursuant to General Assembly resolution 63/185 and Human Rights Council resolution 10/15. The main report lists the activities of the Special Rapporteur from 1 August to 15 December 2009 and focuses thematically on the right to privacy as a human right in the counter-terrorism context. The addenda contain a communications report (A/HRC/13/37/Add.1) and a report on the fact-finding mission to Egypt from 17 to 21 April 2009 (A/HRC/13/37/Add.2).

2. Regarding upcoming country visits, the Special Rapporteur hopes to conduct a mission to Tunisia prior to presenting this report. The Special Rapporteur has suggested dates in late January and early February 2010 and is awaiting a response from the Government. The Special Rapporteur also hopes to conduct official visits to Chile and Peru in 2010. There are outstanding visit requests for Algeria, Malaysia, Pakistan, the Philippines and Thailand.

II. Activities of the Special Rapporteur

3. On 18 and 19 September 2009, the Special Rapporteur convened an expert group meeting at the European University Institute in Florence to discuss thematic issues related to his mandate.¹ The meeting partly coincided with a public event on the "Fight against Terrorism: Challenges for the Judiciary", jointly organized with the Venice Commission and the Sub-Committee on Crime Problems of the Council of Europe. The event was co-funded by the Åbo Akademi University Institute for Human Rights, through its project to support the mandate of the Special Rapporteur.

4. On 29 and 30 September 2009, the Special Rapporteur, along with the other mandate holders involved, participated in informal consultations in Geneva regarding a global joint study on secret detention (A/HRC/13/42). He also met with representatives of the Permanent Missions of Egypt and Tunisia in regard to country visits conducted or planned.

5. On 2 and 3 October 2009, the Special Rapporteur participated in a Wilton Park Conference on "Terrorism, security and human rights: opportunities for policy change" and was a panellist for the discussion on the role of international organizations in response to terrorism and the protection of human rights.

6. On 4 October 2009, the Special Rapporteur delivered a keynote address on the occasion of the inauguration of the academic year at the Faculty of Law at the University of the Basque Country (Universidad del País Vasco) in Bilbao, Spain.

7. From 12 to 14 October 2009, the Special Rapporteur participated in two events in Vienna: the International Workshop of National Counter-Terrorism Focal Points and the Counter-Terrorism Implementation Task Force (CTITF) Retreat. The workshop was jointly organized by a number of member States and the United Nations Office on Drugs and Crime, in close cooperation with the CTITF Office and the Counter-Terrorism Executive Directorate (CTED). It provided a forum to exchange views on how to better link global and national counter-terrorism efforts by fostering greater networking among national

¹ The Special Rapporteur is grateful for the assistance of the members of the expert panel, Dr. Gus Hosein and his research assistant, Mathias Vermeulen, and the participants of his PhD candidate seminar at the European University Institute, in producing this report.

counter-terrorism focal points and facilitating their role as interface between national, regional and global counter-terrorism efforts. The CTITF retreat focused on ways forward to expand and strengthen partnerships between member States, the United Nations system, regional and other organizations and civil society in implementing the United Nations Global Counter-Terrorism Strategy.²

8. On 20 October 2009, the Special Rapporteur was represented at a seminar in Brussels on “Strengthening the UN Targeted Sanctions through Fair and Clear Procedures”, organized by the Belgian Federal Public Service for Foreign Affairs, Foreign Trade and Development Cooperation.

9. From 26 to 28 October 2009, the Special Rapporteur was in New York to present to the Third Committee of the General Assembly his report,³ which focused on the gender impact of counter-terrorism measures. The Special Rapporteur had a formal meeting with the Al-Qaida and Taliban Sanctions Committee of the Security Council and met with the Director of the Counter-Terrorism Executive Directorate (CTED). The Special Rapporteur was a panellist at a side event “Engendering Counter-Terrorism and National Security” hosted by the Centre for Human Rights and Global Justice of the New York University School of Law. He also met with a number of non-governmental organizations and gave a press conference.

10. On 29 October 2009, the Special Rapporteur met with the Assistant Secretary for Democracy, Human Rights and Labor and other officials of the United States State Department in Washington D.C., to discuss current and future legal developments with the new Administration, in follow-up to his visit to the United States of America in 2007,⁴ and more general issues concerning international humanitarian and human rights law in the counter-terrorism context.

III. The right to privacy

A. The right to privacy as enshrined in constitutions and international human rights treaties

11. Privacy is a fundamental human right that has been defined as the presumption that individuals should have an area of autonomous development, interaction and liberty, a “private sphere” with or without interaction with others and free from State intervention and free from excessive unsolicited intervention by other uninvited individuals.⁵ The right to privacy has evolved along two different paths. Universal human rights instruments have focused on the negative dimension of the right to privacy, prohibiting any arbitrary interference with a person’s privacy, family, home or correspondence,⁶ while some regional and domestic instruments have also included a positive dimension: everyone has the right to

² See General Assembly resolution 60/288.

³ A/64/211.

⁴ See A/HRC/6/17/Add.3.

⁵ Lord Lester and D. Pannick (eds.), *Human Rights Law and Practice* (London, Butterworth, 2004), para. 4.82.

⁶ See the Universal Declaration on Human Rights (art. 12); the International Covenant on Civil and Political Rights (ICCPR, art. 17); the International Convention on the Protection of All Migrant Workers and Members of Their Families (art. 14); and the Convention on the Rights of the Child (art. 16).

A/HRC/13/37

respect for his/her private and family life, his/her home and correspondence,⁷ or the right to have his/her dignity, personal integrity or good reputation recognized and respected.⁸ While privacy is not always directly mentioned as a separate right in constitutions, nearly all States recognize its value as a matter of constitutional significance. In some countries, the right to privacy emerges by extension of the common law of breach of confidence, the right to liberty, freedom of expression or due process. In other countries, the right to privacy emerges as a religious value. The right to privacy is therefore not only a fundamental human right, but also a human right that supports other human rights and forms the basis of any democratic society.

12. The State's ability to develop record-keeping facilities was enhanced with the development of information technology. Enhanced computing power enabled previously unimaginable forms of collecting, storing and sharing of personal data. International core data protection principles were developed, including the obligation to: obtain personal information fairly and lawfully; limit the scope of its use to the originally specified purpose; ensure that the processing is adequate, relevant and not excessive; ensure its accuracy; keep it secure; delete it when it is no longer required; and grant individuals the right to access their information and request corrections.⁹ The Human Rights Committee provided clear indications in its general comment No. 16 that these principles were encapsulated by the right to privacy,¹⁰ but data protection is also emerging as a distinct human or fundamental right. Some countries have recognized data protection even as a constitutional right, thereby highlighting its importance as an element of democratic societies. The detailed article 35 of the 1976 Constitution of Portugal can be seen as an example of best practice here.

13. The right to privacy is not an absolute right. Once an individual is being formally investigated or screened by a security agency, personal information is shared among security agencies for reasons of countering terrorism and the right to privacy is almost automatically affected. These are situations where States have a legitimate power to limit the right to privacy under international human rights law. However, countering terrorism is not a trump card which automatically legitimates any interference with the right to privacy. Every instance of interference needs to be subject to critical assessment.

B. Permissible limitations to the right to privacy

14. Article 17 of the International Covenant on Civil and Political Rights is the most important legally binding treaty provision on the human right to privacy at the universal level. The Covenant has been ratified by 165 States and signed by another 6 States.¹¹

⁷ See the European Convention for the Protection of Human Rights and Fundamental Freedoms (art. 8) and the Cairo Declaration on Human Rights in Islam (A/45/421-S/21797, art. 18), 5 August 1990.

⁸ African Charter on Human and People's Rights (art. 11). See also the African Union's Declaration of Principles on Freedom of Expression in Africa (art. 4.3) and the American Declaration of the Rights and Duties of Man (art. 5).

⁹ See the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981; the Organization for Economic Cooperation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980); and the Guidelines for the regulation of computerized personal data files (General Assembly resolution 45/95 and E/CN.4/1990/72).

¹⁰ Human Rights Committee, general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17).

¹¹ As of 16 November 2009. The six countries whose signature has not yet been followed by ratification are China, Cuba, Guinea-Bissau, Nauru, Panama and San Marino.

Article 4 of the Covenant allows States parties to derogate from some provisions of the Covenant, including article 17. Derogations can be made only during a state of emergency threatening the life of the nation and they are subject to several conditions.¹² During the more than 30 years since the entry into force of the Covenant in 1976, fewer than 10 States parties have introduced a state of emergency with reference to acts, or the threat of, terrorism.¹³ Four of them have in that context sought to derogate also from article 17 of the Covenant.¹⁴ Another eight States have announced derogation from article 17 without an explicit reference to terrorism as the cause for a state of emergency.¹⁵ However, the notifications in question have remained rather generic, instead of specifying, in line with the requirements under article 4, what concrete measures derogating from article 17 are necessary within the exigencies of the situation.¹⁶ Overall, there is not a single case of a State seeking to derogate from article 17 with reference to terrorism that would demonstrate compliance with all requirements of article 4. Further, only one State has announced derogation from the Covenant with reference to the current (related to the events of 11 September 2001) threat of international terrorism.¹⁷ The situation is similar in respect of reservations to article 17. Although international law generally allows for reservations by States to human rights treaties, provided such reservations are not incompatible with the object and purpose of the treaty,¹⁸ only one State party has submitted a reservation to article 17.¹⁹

15. Consequently, it appears that States have only rarely resorted to the acknowledged mechanisms available under international law in general, and the Covenant in particular, for unilateral exceptions to the right to privacy. Even when notifications of derogation from article 17 have been submitted, those notifications have remained generic, instead of referring to practical measures and specific forms of derogation. To the Special Rapporteur, the State practice reported above demonstrates that, generally, States appear to be content that the framework of article 17 is flexible enough to enable necessary, legitimate and proportionate restrictions to the right to privacy by means of permissible limitations, including when responding to terrorism. The Special Rapporteur supports this view. Article 17 is written in a manner that allows States parties the possibility to introduce restrictions or limitations in respect of the rights enshrined in that provision, including the right to privacy. Such restrictions and limitations will therefore be subject to the monitoring functions of the Human Rights Committee as the treaty body entrusted with the task of interpreting the provisions of the Covenant and addressing the conduct of States parties in respect of their treaty obligations. The main mechanisms for the exercise of those functions are the mandatory reporting procedure under article 40 of the Covenant and, for those 113 States

¹² For the position of the pertinent treaty monitoring body in respect of the scope and effect of derogations, see Human Rights Committee, general comment No. 29 (2001).

¹³ Azerbaijan, Chile, Colombia, El Salvador, Israel, Nepal, Peru, the Russian Federation and the United Kingdom.

¹⁴ Colombia, El Salvador, Nepal and the Russian Federation.

¹⁵ Algeria, Armenia, Ecuador, Nicaragua, Panama, Serbia and Montenegro, Sri Lanka and the Bolivarian Republic of Venezuela. In some of these cases, there may have been a factual link to terrorism, although this was not mentioned in the notification concerning a state of emergency.

¹⁶ For instance, when seeking to derogate from ICCPR, many Latin American States have plainly notified that some named provisions of the Covenant will be "suspended". This is not in line with the requirements of article 4 as explained in general comment No. 29.

¹⁷ The United Kingdom on 18 December 2001. The derogations did not include article 17 and were withdrawn on 15 March 2005.

¹⁸ For the position of the pertinent treaty monitoring body in respect of reservations to the ICCPR and its optional protocols, see Human Rights Committee, general comment No. 24 (2004).

¹⁹ Liechtenstein maintains a reservation concerning the scope of the right to respect for family life with regard to foreigners.

A/HRC/13/37

that have ratified the First Optional Protocol to the Covenant, the procedure for individual complaints.

16. The wording of article 17 of the Covenant prohibits “arbitrary or unlawful” interference with privacy, family or correspondence, as well as “unlawful attacks” on a person’s honour and reputation. This can be contrasted with the formulation of such provisions as article 12, paragraph 3; article 18, paragraph 3; article 19, paragraph 3; article 21 and article 22, paragraph 2, which all spell out the elements of a test for permissible limitations. In its most elaborate form, this test is expressed in article 21 and article 22, paragraph 3, as consisting of the following three elements: (a) restrictions must be prescribed by national law; (b) they must be necessary in a democratic society; and (c) they must serve one of the legitimate aims enumerated in each of the provisions that contain a limitations clause.

17. The Special Rapporteur takes the view that, despite the differences in wording, article 17 of the Covenant should also be interpreted as containing the said elements of a permissible limitations test. Restrictions that are not prescribed by law are “unlawful” in the meaning of article 17, and restrictions that fall short of being necessary or do not serve a legitimate aim constitute “arbitrary” interference with the rights provided under article 17. Consequently, limitations to the right to privacy or other dimensions of article 17 are subject to a permissible limitations test, as set forth by the Human Rights Committee in its general comment No. 27 (1999). That general comment addresses freedom of movement (art. 12), one of the provisions that contains a limitations clause. At the same time, it codifies the position of the Human Rights Committee in the matter of permissible limitations to the rights provided under the Covenant. The permissible limitations test, as expressed in the general comment, includes, *inter alia*, the following elements:

- (a) Any restrictions must be provided by the law (paras. 11–12);
- (b) The essence of a human right is not subject to restrictions (para. 13);
- (c) Restrictions must be necessary in a democratic society (para. 11);
- (d) Any discretion exercised when implementing the restrictions must not be unfettered (para. 13);
- (e) For a restriction to be permissible, it is not enough that it serves one of the enumerated legitimate aims; it must be necessary for reaching the legitimate aim (para. 14);
- (f) Restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve the desired result; and they must be proportionate to the interest to be protected (paras. 14–15);
- (g) Any restrictions must be consistent with the other rights guaranteed in the Covenant (para. 18).²⁰

18. The Special Rapporteur takes the view that these considerations apply also in respect of article 17 of the Covenant, as elaborations of the notions of “unlawful” and “arbitrary”. Where the textual difference between article 17 and the Covenant provisions that explicitly introduce a limitations test nevertheless matters is in the absence of an exhaustive list of legitimate aims in article 17. Here, the Special Rapporteur calls upon States to justify why a particular aim is legitimate as justification for restrictions upon article 17, and upon the Human Rights Committee to continue monitoring measures undertaken by States parties, including through the consideration of periodic reports and of individual complaints.

²⁰ See Human Rights Committee, general comment No. 27 (1999).

19. In the view of the Special Rapporteur, the Human Rights Committee should draw up and adopt a new general comment on article 17, replacing current general comment No. 16 (1988). The existing general comment is very brief and does not reflect the bulk of the Committee's practice that has emerged during the more than 20 years since its adoption. Nevertheless, many of the elements for a proper limitations clause, presented above in the light of the subsequent general comment No. 27, were already present in 1988.²¹ In its subsequent case law under the Optional Protocol, the Committee has emphasized that interference with the rights guaranteed in article 17 must cumulatively meet several conditions, i.e., it must be provided for by law, be in accordance with the provisions, aims and objectives of the Covenant, and be reasonable in the particular circumstances of the case.²² Further, in finding violations of article 17, the Committee has applied the requirements of legitimate aim, necessity and proportionality.²³

C. Erosion of the right to privacy by counter-terrorism policies

20. When considering current counter-terrorism policies, States often contend that there are two new dynamics that must be considered alongside privacy protection. First, States claim that their ability to prevent and investigate terrorist acts is linked intimately with increased surveillance powers. The majority of counter-terrorism legislation activities since the events of 11 September 2001 have therefore focused on expanding Governments' powers to conduct surveillance. Second, States claim that since terrorism is a global activity, the search for terrorists must also take place beyond national borders, with the help of third parties which potentially hold extensive amounts of information on individuals, generating a rich resource for identifying and monitoring terrorist suspects. States that previously lacked constitutional or statutory safeguards have been able to radically transform their surveillance powers with few restrictions. In countries that have constitutional and legal safeguards, Governments have endangered the protection of the right to privacy by not extending these safeguards to their cooperation with third countries and private actors, or by placing surveillance systems beyond the jurisdiction of their constitutions.

1. Increasing surveillance measures

21. The range of surveillance operations runs from the specific to the general. At the specific level, legal systems are capable of authorizing and overseeing: undercover operations and covert surveillance to identify illegal conduct; the accumulation of intelligence on specific individuals to identify breaches of law; and targeted surveillance of individuals to build a legal case. The Special Rapporteur had earlier specified that States may make use of targeted surveillance measures, provided that it is case-specific interference, on the basis of a warrant issued by a judge on showing of probable cause or reasonable grounds. There must be some factual basis, related to the behaviour of an individual, which justifies the suspicion that he or she may be engaged in preparing a terrorist attack.²⁴ Worldwide, there has been a rise in communications surveillance through the interception of communications by intelligence and law enforcement agencies. There is a remarkable convergence in the types of policies pursued to enhance surveillance powers

²¹ See Human Rights Committee, general comment No. 16 (1988). See, in particular, paragraphs 3 and 4 that elaborate upon the notions of arbitrary and unlawful interference in ICCPR, art. 17.

²² See *Van Hulst v. The Netherlands*, communication No. 903/1999, 2004.

²³ See *Madafferi v. Australia*, communication No. 1011/2001, 2004, and *M.G. v. Germany*, communication No. 1482/2006, 2008.

²⁴ A/HRC/10/3, para. 30.

A/HRC/13/37

to respond to terrorism threats. Most of these policies rely upon existing or new technologies, such as “bugs” and tracing technologies that can access the geographical position of mobile phones, technology that reports to Governments the contents of private text conversations of users of voice over Internet protocol,²⁵ or that installs spyware on suspects’ computers in order to enable remote computer access.²⁶ In some countries, security services have even proposed banning communication technologies that are more difficult to intercept, such as smartphones.²⁷ The Special Rapporteur is also concerned about the tracking of cross-border communications without judicial authorization.²⁸

22. In the name of countering terrorism, States have expanded initiatives to identify, scan and tag the general public through the use of multiple techniques which might violate an individual person’s right to privacy. When surveillance occurs of places and larger groups of people, the surveillance is typically subject to weaker regimes for authorization and oversight. Human rights standards have been tested, stretched and breached through the use of stop-and-searches; the compilation of lists and databases; the increased surveillance of financial, communications and travel data; the use of profiling to identify potential suspects; and the accumulation of ever larger databases to calculate the probability of suspicious activities and identify individuals seen as worthy of further scrutiny. More advanced techniques are applied as well, such as the collection of biometrics or the use of body scanners that can see through clothing.²⁹ Some intrusions into people’s lives can be permanent as people’s physical and biographical details are frequently centralized in databases.

(a) *Stop and search powers*

23. States have expanded their powers to stop, question, search and identify individuals, and have reduced their controls to prevent abuse of these powers. These powers have given rise to concerns regarding racial profiling and discrimination in Europe³⁰ and the Russian Federation³¹ and concerns that these powers antagonize the relationship between citizens and the State. Equally, the proportionality requirement in the limitations test to the right to privacy raises questions whether blanket stop and search powers in designated security zones, such as in the Russian Federation³² or the United Kingdom,³³ are really necessary in a democratic society.

(b) *The use of biometrics and dangers of centralized identity systems*

24. A key component to new identity policies is the use of biometric techniques, such as facial recognition, fingerprinting and iris-scanning. While these techniques can, in some circumstances, be a legitimate tool for the identification of terrorist suspects, the Special

²⁵ D. O’Brien, “Chinese Skype client hands confidential communications to eavesdroppers”, Electronic Frontier Foundation, 2 October 2008.

²⁶ See the article at the following address: http://www.bundestag.de/dokumente/textarchiv/2008/22719940_kw46_bka/index.html.

²⁷ S. Das Gupta and L. D’Monte, “BlackBerry security issue makes e-com insecure”, *Business Standard*, 12 March 2008.

²⁸ See, for instance, the Swedish Government’s bill on adjusted defence intelligence operations, adopted in June 2008, p. 83.

²⁹ See the European Parliament resolution of 23 October 2008 on the impact of aviation security measures and body scanners on human rights, privacy, personal dignity and data protection.

³⁰ Open Society Justice Initiative, *Ethnic Profiling by Police in Europe*, June 2005.

³¹ Open Society Justice Initiative and JURIX, *Ethnic Profiling in the Moscow Metro*, June 2006.

³² 2006 Federal Act No. 35 on Counteraction of Terrorism.

³³ See, e.g., United Kingdom Appeal Court, *R. v. Commissioner of Police for the Metropolis and another*, 2006.

Rapporteur is particularly concerned about cases where biometrics are not stored in an identity document, but in a central database, thereby increasing the information security risks and leaving individuals vulnerable. As the collection of biometric information increases, error rates may rise significantly.³⁴ This may result in the wrongful criminalization of individuals or social exclusion. Meanwhile, unlike other identifiers, biometrics cannot be revoked: once copied and/or fraudulently used by a malicious party, it is not possible to issue an individual with a new biometric signature.³⁵ In this context, it has to be noted that, contrary to its scientific objectivity, DNA evidence can also be falsified.³⁶

25. Centralized collection of biometrics creates a risk of causing miscarriages of justice, which is illustrated by the following example. Following the Madrid bombings of 11 March 2004, the Spanish police managed to lift a fingerprint from an unexploded bomb. Fingerprint experts from the United States Federal Bureau of Investigation (FBI) declared that a lawyer's fingerprint was a match to the crime-scene sample. The person's fingerprint was on the national fingerprint system because he was a former soldier of the United States. The individual was detained for two weeks in solitary confinement, even though the fingerprint was not his. Examiners failed to sufficiently reconsider the match, a situation that was made worse for him when it was discovered that he, as a lawyer, had defended a convicted terrorist, was married to an Egyptian immigrant, and had himself converted to Islam.³⁷

(c) *The circulation of secret watch lists*

26. Another available technique is watch-list monitoring. The most common type of watch-list monitoring is the "no-fly/selectee" list. Such lists are circulated to airlines and security officials with instructions to detain and question any passenger with a certain name. Little is known of the extent to which these lists are being used, but where these systems are publicly overseen, a number of errors and privacy concerns have arisen, particularly in the United States³⁸ and Canada.³⁹ Data integrity issues remain, as the lists have to be continually checked for errors and the identification processes must be performed with great care. These lists are frequently kept secret as they could tip off suspected terrorists, but at the same time this secrecy gives rise to problems of individuals being continually subject to scrutiny without knowing that they are on some form of list, and without effective independent oversight. Such secret surveillance could constitute a violation of the right to privacy under article 17 of the International Covenant on Civil and Political Rights.

27. Where terrorist lists have been made public, article 17 of the Covenant is triggered in another form. The Human Rights Committee has concluded that the unjustified inclusion of a person on the United Nations 1267 Committee's Consolidated List constituted a violation of article 17. It considered that the dissemination of personal information

³⁴ See, for example, M. Cherry and E. Imwinkelried, "A cautionary note about fingerprint analysis and reliance on digital technology", *Judicature*, vol. 89, No. 6 (2006).

³⁵ See E. Kosta et al., "An analysis of security and privacy issues relating to RFID enabled ePassports", *International Federation for Information Processing*, No. 232 (2007), pp. 467-472.

³⁶ See, for example, D. Frumkin et al., "Authentication of forensic DNA samples" *Forensic Science International: Genetics* (17 July 2009).

³⁷ See the United States Department of Justice, Office of the Inspector General, *A Review of the FBI's Handling of the Brandon Mayfield Case*, January 2006.

³⁸ See the United States Department of Justice, *Audit of the FBI Terrorist Watchlist Nomination Practices*, May 2009.

³⁹ See the Office of the Privacy Commissioner Canada, *Audit of the Passenger Protect Program of Transport Canada*, November 2009.

A/HRC/13/37

constituted an attack on the honour and reputation of the listed persons, in view of the negative association that would be made between the names and the title of the sanctions list.⁴⁰

28. Public and secret watch lists often also breach fundamental principles of data protection. Information generated for one purpose is reused for secondary purposes, and sometimes shared with other institutions, without the knowledge or consent of the individuals concerned. Erroneous information is used to make decisions about people, which result in restrictions on travel. These individuals may be refused a visa, turned away at a border or prevented from boarding a plane, without having been presented with evidence of any wrongdoing.

(d) *Checkpoints and borders*

29. Through the use of new technologies and in response to rising concerns regarding terrorism, States are increasing the monitoring, regulation, interference and control of the movement of people at borders. Now, with the use of more advanced technologies and data-sharing agreements, States are creating comprehensive profiles on foreign travellers to identify terrorists and criminals even in advance of their arrival at borders, by accessing passenger manifests and passenger reservation records from carriers. States analyse this information to identify patterns that correspond to those of terrorists or criminals. At the border, individuals are subjected to further — potentially invasive — information collection practices.

30. Many States now require carriers to submit passenger manifests prior to departure. States are also seeking access to passenger name records, which include identification information (name, telephone number), transactional information (dates of reservations, travel agent, itineraries), flight and seat information, financial data (credit card number, invoice address), choice of meals and information regarding place of residence, medical data, prior travel information, and frequent-flyer information. This information is used for profiling and risk-assessing passengers, usually by submitting queries to various multi-agency law enforcement and terrorist databases and watch lists. As a result, foreign carriers may be restricted from issuing an individual with a boarding pass solely on the basis of the results of a database query in the destination country, without due process.

31. The increased monitoring of immigrants and travellers for various purposes gives rise to a number of privacy challenges. States are gaining information on travellers from third parties who are compelled to comply lest they be refused landing rights or given punitive fines, even though privacy guarantees may not meet the requirements of domestic privacy laws. Moreover, foreigners might not be granted equal access to judicial remedies in these countries and rights at borders are usually significantly restricted. The United States Government policy on access to travellers' laptops is a useful example. Despite the need to meet constitutional due process requirements for searching a laptop within the United States, the Department of Homeland Security has approved the accessing of travellers' computers without judicial authorization.⁴¹

32. Lastly, States are establishing additional information requirements. Individuals can be prevented from entering States for refusing to disclose information, and States may insist upon disclosure without ensuring that there is lawful authority to require this information. Additionally, information collected for one purpose is now being used for additional purposes; for example, the European Union's European Dactyloscopic system

⁴⁰ See Human Rights Committee, communication No. 1472/2006, paras. 10.12–10.13.

⁴¹ See the Department of Homeland Security, *Privacy impact assessment for the border searches of electronic devices*, 25 August, 2009.

(EURODAC) for managing applications of asylum-seekers and illegal immigrants through the use of fingerprints is now proposed to be extended to aid the prevention, detection, and investigation of terrorist offences and other serious offences. The European Data Protection Supervisor has expressed doubts as to whether these proposals are legitimate under the right to privacy.⁴²

2. How surveillance has affected other rights

33. Surveillance regimes adopted as anti-terrorism measures have had a profound, chilling effect on other fundamental human rights. In addition to constituting a right in itself, privacy serves as a basis for other rights and without which the other rights would not be effectively enjoyed. Privacy is necessary to create zones to allow individuals and groups to be able to think and develop ideas and relationships. Other rights such as freedom of expression, association, and movement all require privacy to be able to develop effectively. Surveillance has also resulted in miscarriages of justice, leading to failures of due process and wrongful arrest.

34. In many nations around the world, users are being monitored to review what sites they are visiting and with whom they are communicating. In Germany, the Federal Intelligence Service was found in 2006 to have been illegally spying on journalists using communications surveillance and placing spies in newsrooms.⁴³ In Colombia, the Administrative Department of Security was found, in 2009, to have been conducting illegal surveillance of members of the media, human rights workers, Government officials and judges, and their families for seven years.⁴⁴ In numerous countries across the world, internet users must show identification and their sessions are recorded for future use by authorities. For instance, in Internet service providers in Bangladesh were required in 2007 to turn over records of their users' identities, passwords and usage to the authorities. Some users were then visited by the authorities, who searched through their computers and contact lists.⁴⁵ In the United States, the FBI counter-terrorism unit monitored the activities of peace activists at the time of the 2004 political conventions.⁴⁶ These surveillance measures have a chilling effect on users, who are afraid to visit websites, express their opinions or communicate with other persons for fear that they will face sanctions.⁴⁷ This is especially relevant for individuals wishing to dissent and might deter some of these persons from exercising their democratic right to protest against Government policy.

35. In addition to surveillance powers, many anti-terrorism laws require individuals to proactively disclose information and provide broad powers for officials to demand information for investigations. In this context, the Special Rapporteur has earlier expressed his concerns about the use of national security letters in the United States.⁴⁸ Some countries have expanded this power to require the disclosure of information originally collected for journalistic purposes. In Uganda, the 2002 Anti-Terrorism Act allows for wiretapping and

⁴² See the statement by the European Data Protection Supervisor on law enforcement access to EURODAC, 8 October 2009.

⁴³ Deutsche Welle World, "Germany stops journalist spying in wake of scandal", 15 May 2006.

⁴⁴ See *Semana*, 21 February 2009.

⁴⁵ See *E-Bangladeshi*, "Crackdown on internet users in Bangladesh", 3 October 2007 (translating BBC reports).

⁴⁶ See the American Civil Liberties Union, "ACLU uncovers FBI Surveillance of main peace activists", 25 October 2006.

⁴⁷ See D.S. Sidhu, "The chilling effect of government surveillance programs on the use of the Internet by Muslim-Americans", *University of Maryland Law Journal of Race, Religion, Gender and Class*, vol. 7 (2007), p. 375.

⁴⁸ A/HRC/6/17/Add.3, para. 51.

A/HRC/13/37

searches of the media if there are “special reasonable grounds” that the information has “substantial value” in an anti-terrorism investigation.⁴⁹ The Special Rapporteur stresses that the legitimate interest in the disclosure of confidential materials of journalists outweighs the public interest in the non-disclosure only where an overriding need for disclosure is proved, the circumstances are of a sufficiently vital and serious nature and the necessity of the disclosure is identified as responding to a pressing social need.⁵⁰

36. The rights to freedom of association and assembly are also threatened by the use of surveillance. These freedoms often require private meetings and communications to allow people to organize in the face of Governments or other powerful actors. Expanded surveillance powers have sometimes led to a “function creep”, when police or intelligence agencies have labelled other groups as terrorists in order to allow the use of surveillance powers which were given only for the fight against terrorism. In the United States, environmental and other peaceful protestors were placed on terrorist watch lists by the Maryland State Police before political conventions in New York and Denver.⁵¹ In the United Kingdom, surveillance cameras are commonly used for political protests and images kept in a database.⁵² A recent poll in the United Kingdom found that one third of individuals were disinclined to participate in protests because of concern about their privacy.⁵³

37. Freedom of movement can also be substantially affected by surveillance. The creation of secret watch lists, excessive data collection and sharing and imposition of intrusive scanning devices or biometrics, all create extra barriers to mobility. As described in previous sections, there has been a substantial increase in the collection of information about people travelling both nationally and internationally. Information is routinely shared and used to develop watch lists that have led to new barriers to travel. When profiles and watch lists are developed using information from a variety of sources with varying reliability, individuals may have no knowledge of the source of the information, may not question the veracity of this information, and have no right to contest any conclusions drawn by foreign authorities. A mosaic of data assembled from multiple databases may cause data-mining algorithms to identify innocent people as threats.⁵⁴ If persons are prohibited from leaving a country, the State must provide information on the reasons requiring the restriction on freedom of movement. Otherwise, the State is likely to violate article 12 of the International Covenant on Civil and Political Rights.⁵⁵

38. One of the most serious effects of surveillance measures is that they may lead to miscarriages of justice and violate due process guarantees. The challenge of gaining access to judicial review is that some legal regimes may prevent access to the courts unless individuals can show that interference has taken place, which is precluded by the secretive

⁴⁹ Anti-terrorism Act, third schedule, para. 8.

⁵⁰ See also recommendation No. R (2000) 7, of the Council of Europe Committee of Ministers to member States on the right of journalists not to disclose their sources of information and Ontario Superior Court of Justice, *O'Neill v. Canada (Attorney General)*, 2006, para. 163.

⁵¹ See L. Rein and J. White, “More groups than thought monitored in police spying”, *The Washington Post*, 4 January 2009.

⁵² See P. Lewis and M. Vallée, “Revealed: police databank on thousands of protesters”, *The Guardian*, 6 March 2009.

⁵³ See A. Jha and J. Randerson, “Poll shows public disquiet about policing at environmental protests”, *The Guardian*, 25 August 2009.

⁵⁴ See United States National Research Council, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Assessment, Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals*, October 2008.

⁵⁵ See, similarly, Human Rights Committee, *B. Zoolfia v. Uzbekistan*, communication No. 1585/2007, 2009, para. 8.3.

nature of the surveillance programmes. Individuals may not be able to prove or demonstrate that they are actually under surveillance. As a result, individuals may not be able to appeal to courts for remedy. In relevant cases, courts have ruled that individuals lack standing because they cannot demonstrate that they were under surveillance and any injuries have been considered speculative.⁵⁶ In other cases, where interference can be proven, States have sometimes applied the “State secrets” privilege to avoid scrutiny of illegal surveillance projects.⁵⁷ The Special Rapporteur commends the approach of the European Court of Human Rights (ECHR) where individuals do not need to prove that such measures necessarily had applied to them.⁵⁸

3. Extending legal boundaries

39. Mutual legal assistance treaties are established to permit countries to cooperate in investigations and to share information in specific cases.⁵⁹ Agreements have also been established to permit the sharing of information on individuals engaged in activities, e.g., all passengers travelling to another country or all individuals conducting interbank financial transactions. More opaque are the agreements between intelligence agencies to share databases and intelligence data. These databases are often subject to wide-ranging exemptions from the domestic legal system. Even if domestic legislation applies, the data may refer to foreign nationals who may not be permitted to exercise any rights in domestic courts. Individuals may not be aware of the fact that they are subject to surveillance — e.g., that they are on a list of suspected terrorists — because intelligence-driven lists are not publicly available and therefore they may not appeal for review. When that list is shared internationally individuals may not be able to identify why they were first placed on it, or otherwise be able to remove themselves from the multiplicity of lists that have emerged since then.

40. States have increased not only their cooperation with each other in the fight against terrorism, but also with private third parties that have personal information of individuals in order to identify and monitor terrorist suspects. Some Governments have subsequently endangered the protection of the right to privacy by not extending domestic privacy safeguards to their cooperation with third countries and private actors.

41. Third parties, such as banks, telephone companies or even cybercafes, now hold extensive personal information about individuals. Access to this information therefore provides significant details about the private lives of individuals. At the same time, government agencies may gain access to this information with fewer restrictions than if the information was held by individuals themselves, in the home, or even by other government agencies. In the United States, for instance the Supreme Court has ruled that, as data provided to third parties such as banks or telephone companies is shared “freely” with these parties, individuals may not reasonably expect privacy.⁶⁰ Where there is a lack of constitutional protections that require a legal basis for the interference in the private lives of individuals, the burden then falls on the private organization to decide how to respond to a request from a government agency. Generally, the private sector prefers that Governments

⁵⁶ This was most recently concluded in *Amnesty International et al. v. John McConnell et al.*, United States District Court for the Southern District of New York, 20 August 2009.

⁵⁷ See United States District Court for the Northern District of California, *Al-Haramain Islamic Foundation et al. v. Bush et al.*, 1 May 2009.

⁵⁸ See ECHR, *Klass v. Germany*, 6 September 1978, para. 38.

⁵⁹ See G. Hosein, *International Co-operation as a Promise and a Threat, in Cybercrime and Jurisdiction: A Global Survey* (T.M.C. Asser Press), 2006.

⁶⁰ See United States Supreme Court, *Smith v. Maryland*, 1979, in the case of communications data, and *United States v. Miller*, 1976, in the case of financial information.

establish a legal basis for obliging organizations to produce personal information upon request, as it removes their obligation to consider the nature of the case.

42. Third parties are also increasingly being called upon to collect more information than is necessary, and to retain this information for extended periods of time. The United Kingdom, for instance, has proposed that telecommunications companies actively monitor and retain information on individuals' online activities including social-networking activities – information that these companies have no justified interest in collecting.⁶¹ Similarly, the European Union's data retention directive⁶² has generated considerable criticism. When, in 2008, the German Federal Constitutional Court temporarily suspended the German law implementing that directive, it noted that “the retention of sensitive data, comprehensive and without occasion, on virtually everyone, for Government purposes that at the time of the storage of the data cannot be foreseen in detail, may have a considerable intimidating effect”.⁶³ Also in Germany, research showed a chilling effect of data retention policies: 52 per cent of persons interviewed said they probably would not use telecommunication for contact with drug counsellors, psychotherapists or marriage counsellors because of data retention laws.⁶⁴

43. In this context, the Special Rapporteur is concerned that, in many countries, data retention laws have been adopted without any legal safeguards over the access to this information being established or without the fact that new technological developments are blurring the difference between content and communications data being considered. While constitutional provisions tend to require safeguards on access to communications content, the protection of transaction logs is more limited. While this information may be integral to investigations, it may also be just as privacy-sensitive as the content of communications transactions.

44. With the goal of combating terrorism financing and money laundering, States have obliged the financial industry to analyse financial transactions in order to automatically distinguish those “normal” from those “suspicious”. For instance, the European Union established a directive in 2005 on “the prevention of the use of the financial system for the purpose of money laundering and terrorist financing”⁶⁵ requiring that financial institutions follow due diligence by reporting suspicious and “threshold” activities to financial intelligence units (FIUs). The additional processing of this information by the FIUs remains opaque, but States like Australia⁶⁶ and Canada⁶⁷ are processing millions of transactions each year through advanced data-mining tools.

45. Third parties may also be subject to foreign laws requiring disclosure. The United States Government, for instance, issued administrative subpoenas to the Society for

⁶¹ See British All Party Parliamentary Group on Privacy, *Briefing Paper: Inquiry into communications data surveillance proposals and the Interception Modernisation Programme*, June 2009.

⁶² Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *Official Journal*, L 105 (2006), pp. 54–63.

⁶³ Constitutional Court decision No. 256/08, 11 March 2008.

⁶⁴ German Forsa Institute, *Meinungen der Bunderburger zur Vorratsdatenspeicherung*, 28 May 2008.

⁶⁵ See Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, *Official Journal*, L 309 (2005), pp. 15–36.

⁶⁶ See Australian Transaction Reports and Analysis Centre, *AUSTRAC Annual Report 2008–09*, October 2009.

⁶⁷ See Financial Transaction and Reports Analysis Centre of Canada, *FINTRAC Annual Report 2008*, 11 September 2008.

Worldwide Interbank Financial Telecommunication (SWIFT), the Belgian cooperative responsible for enabling messaging between more than 7,800 financial institutions in over 200 countries. By gaining access to the SWIFT data centre in the United States, the country's Treasury was then able to monitor foreign financial transactions across the SWIFT network, to find and identify terrorist suspects.⁶⁸ Human rights groups filed legal complaints in over 20 courts arguing that, by handing this information over to United States authorities, SWIFT was in breach of local privacy laws.⁶⁹

46. The Special Rapporteur is also concerned that surveillance is being embedded in technological infrastructures, and that these will create risks for individuals and organizations. For example, the development of standards for lawful interception of communications requires telecommunications companies to design vulnerabilities into their technologies to ensure that States may intercept communications. These capabilities were abused in Greece where unknown third parties were able to listen to the communications of the Prime Minister of Greece, and dozens of other high-ranking dignitaries.⁷⁰ More recently, these same capabilities were reported to have been used by the Government of the Islamic Republic of Iran to monitor protestors.⁷¹ To avoid abuse, surveillance technologies should log who accesses data, thereby leaving a trail that can itself be monitored for abuse.⁷²

47. In some States, constitutional safeguards continue to apply, however. In Canada, for example, the Charter of Rights and Freedoms protects privacy of information held by third parties when it reveals "intimate details of the lifestyle and personal choices of the individual".⁷³ This requires balancing of the societal interests in protecting individual dignity, integrity and autonomy with effective law enforcement.⁷⁴ The jurisprudence of the European Convention of Human Rights has similarly extended the right to privacy to information held by third parties. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data requires both the public and private sectors to protect the information that they hold and regulates the sharing of information with government agencies. Exceptions apply when protecting State security, public safety or the monetary interests of the State, suppressing criminal offences or protecting individuals or the rights and freedoms of others.⁷⁵

D. Best practices

48. The Special Rapporteur is concerned that there is a trend towards extending such State surveillance powers beyond terrorism. Following the events of 11 September 2001, a number of legislatures introduced sunset clauses into and reviews of anti-terrorism legislation, as it was assumed that extraordinary powers may be required for a short period of time to respond to the then danger. These sunset clauses and reviews were not included

⁶⁸ See also the statement of United States Under Secretary Stuart Levey on the Terrorist Finance Tracking Program, 23 June 2006.

⁶⁹ See, for example, Privacy International, "Pulling a Swift one? Bank transfer information sent to U.S. authorities", 27 July 2006.

⁷⁰ See, for background, V. Prevelakis and D. Spinellis, "The Athens Affair", *IEEE Spectrum*, July 2007.

⁷¹ See, for reference, Nokia Siemens Networks, "Provision of lawful intercept capability in Iran", 22 June 2009.

⁷² See footnote 54.

⁷³ See Supreme Court of Canada, *R. v. Plant*, 1993, and *R. v. Tessling*, 2004.

⁷⁴ *R. v. Plant*.

⁷⁵ Article 9 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

A/HRC/13/37

in some areas of policymaking and, in later policies, were not considered at all. Many of the investigative powers given to law enforcement agencies under anti-terror laws are granted to these agencies to conduct investigations unrelated to terrorism. Meanwhile, States are following each other's lead on policy without considering the human rights implications. Many of the policies outlined above were introduced first as extraordinary, but then soon became regional and international standards. Collectively, such interference is having significant negative impacts on the protection of the right to privacy, as there is limited access to legal safeguards. Without a rigorous set of legal safeguards and a means to measure the necessity, proportionality, or reasonableness of the interference, States have no guidance on minimizing the risks to privacy generated by their new policies. The Special Rapporteur has identified the legal safeguards that have emerged through policymaking, jurisprudence, policy reviews and good practice from around the world.

1. The principle of minimal intrusiveness

49. Some interference with the private lives of individuals is more intrusive than others. Constitutional protection of property and people has been extended over the past 50 years to include communications,⁷⁶ information that is related to a biographical core⁷⁷ and a right to the confidentiality and integrity of information-technological systems.⁷⁸ These protections require States to have exhausted less-intrusive techniques before resorting to others. The United Kingdom Parliament's Home Affairs Committee reviewed and adapted these ideas for modern data-centred surveillance systems into the principle of data-minimization, which is closely linked to purpose-specification.⁷⁹ In its review, the Parliamentary committee recommended that Governments "resist a tendency to collect more personal information and establish larger databases. Any decision to create a major new database, to share information on databases, or to implement proposals for increased surveillance, should be based on a proven need". The Special Rapporteur contends that States must incorporate this principle into existing and future policies as they present how their policies are necessary, and in turn proportionate.

2. The principle of purpose specification restricting secondary use

50. Whereas data protection law should protect information collected for one purpose being used for another, national security and law enforcement policies are generally exempted from these restrictions. This is done through secrecy provisions in lawful access notices, broad subpoenas and exemption certificates such as national security certificates, which exempt a specific database from adhering to privacy laws. The Special Rapporteur is concerned that this limits the effectiveness of necessary safeguards against abuse. States must be obliged to provide a legal basis for the reuse of information, in accordance with constitutional and human rights principles. This must be done within the human rights framework, rather than resorting to derogations and exemptions. This is particularly important when information is shared across borders; furthermore, when information is shared between States, protections and safeguards must continue to apply.⁸⁰

⁷⁶ See United States Supreme Court, *Katz v. United States*, 1967.

⁷⁷ See footnote 74.

⁷⁸ See German Constitutional Court decision No. 370/07, 27 February 2008.

⁷⁹ See the United Kingdom Parliament's Home Affairs Committee, *A Surveillance Society? Fifth report of the session 2007–2008*, 8 June 2008.

⁸⁰ See, for instance, with regard to passenger name records, the article 29 Data Protection Working Party's opinion 8/2004 on the information for passengers concerning the transfer of PNR data on flights between the European Union and the United States of America, 30 September 2004.

3. The principle of oversight and regulated authorization of lawful access

51. Surveillance systems require effective oversight to minimize harm and abuses. Where safeguards exist, this has traditionally taken the form of an independent authorization through a judicial warrant and/or a subpoena process with the opportunity of independent review. Many policies have attempted to restrict oversight and lower authorization levels, however: communications interception laws have minimized authorization requirements for some communications; secret subpoenas are issued to gain access to information held by third parties and have restricted the ability to seek judicial protections; and States are increasingly allowing intelligence and law enforcement agencies to self-authorize access to personal information where previously some form of independent authorization and effective reporting was necessary.

52. Some States have taken measures to address the erosion of safeguards. In the United States, after a number of court cases and because of the reauthorization requirements under the USA Patriot Act, more opportunities for judicial review have been reintroduced. Changes to the communications surveillance practices in Sweden and the United States have reintroduced some limited safeguards in the form of judicial warrants. Similarly, the European Court of Justice ruled that courts had to review the domestic lawfulness of international watch lists.⁸¹

53. The Special Rapporteur is concerned that the lack of effective and independent scrutiny of surveillance practices and techniques calls into question whether interferences are lawful (and thus accountable) and necessary (and thus applied proportionately). He commends the hard work of oversight bodies within government agencies, including internal privacy offices, audit departments and inspectorate-generals, as they too play a key role in identifying abuses. The Special Rapporteur therefore calls for increased internal oversight to complement the processes for independent authorization and external oversight. This internal and external accountability system will ensure that there are effective remedies for individuals, with meaningful access to redress mechanisms.

4. The principle of transparency and integrity

54. The application of secrecy privileges for surveillance systems inhibits the ability of legislatures, judicial bodies and the public to scrutinize State powers. Individuals may be subject to inappropriate surveillance, where profiles are developed through data mining, and erroneous judgements, without any prior notification of the practice. Furthermore, the lack of clear and appropriate limitations to surveillance policies makes it difficult to prove that these powers are not used in arbitrary and indiscriminate manners.

55. The principle of transparency and integrity requires openness and communication about surveillance practices. In some States, individuals must be notified when and how they are under surveillance, or as soon as possible after the fact. Under *habeas data* constitutional regimes in Latin America⁸² and European data protection laws, individuals must be able to gain access to and correct their personal information held within data stores and surveillance systems. These rights must be ensured across borders by ensuring that legal regimes protect citizens and non-citizens alike.

56. Open debate and scrutiny is essential to understanding the advantages and limitations of surveillance techniques, so that the public may develop an understanding of

⁸¹ *Yassin Abdullah Kadi and Al Barakaat International Foundation v. Council and Commission*, September 2008.

⁸² See, e.g., Constitution of Brazil, art. 5 (LXXI); Constitution of Paraguay, art. 135; Constitution of Argentina, art. 43.

A/HRC/13/37

the necessity and lawfulness of surveillance. In many States, parliaments and independent bodies have been charged with conducting reviews of surveillance policies and procedures, and on occasion have been offered the opportunity for pre-legislative review. This has been aided by the use of sunset and review clauses in legislation.

5. The principle of effective modernization

57. Even as more invasive information is available with greater ease, States have not developed commensurate protection. In fact, in the name of modernizing their surveillance powers, States sometimes have intentionally sought to apply older and weaker safeguard regimes to ever more sensitive information.⁸³ Conscious of the need to consider how technology and policy change may have a negative impact on individuals, some States have introduced privacy impact assessments that articulate privacy considerations in the design of new surveillance techniques, including how policymakers considered many of the principles listed above, including data minimization and rights to redress. The Special Rapporteur believes that the use of such tools as privacy impact assessments may help inform the public about surveillance practices, while instilling a culture of privacy within government agencies as they develop new surveillance systems to combat terrorism. International standards must also be adopted to require States to enhance their safeguards to reflect technological change.

IV. Conclusions and recommendations

A. Conclusions

58. **The Special Rapporteur is concerned that what was once exceptional is now customary. First, States no longer limit exceptional surveillance schemes to combating terrorism and instead make these surveillance powers available for all purposes. Second, surveillance is now engrained in policymaking. Critics of unwarranted surveillance proposals must now argue why additional information must not be collected, rather than the burden of proof residing with the State to argue why the interference is necessary. Third, the quality and effectiveness of nearly all legal protections and safeguards are reduced. This is occurring even as technological change allows for greater and more pervasive surveillance powers. Most worrying, however, is that these technologies and policies are being exported to other countries and often lose even the most basic protections in the process.**

59. **International legal standards must be developed to ensure against these forms of abuse. This would be aided by adherence to principles outlined in this report, including ensuring that surveillance is as unintrusive as possible and that new powers are developed with appropriate safeguards and limitations, effective oversight and authorization and regular reporting and review and are accompanied by comprehensive statements regarding the impact on privacy. The general public and legislatures have rarely had the opportunity to debate whether anti-terrorism powers are necessary, proportionate or reasonable. The Special Rapporteur believes that following emergent good practices may prove beneficial to all.**

⁸³ See the Policy Engagement Network, *Briefing on the UK Government's Interception Modernisation Programme*, June 2009.

B. Recommendations

For legislative assemblies

60. The Special Rapporteur recommends again that any interference with the right to privacy, family, home or correspondence should be authorized by provisions of law that are publicly accessible, particularly precise and proportionate to the security threat, and offer effective guarantees against abuse. States should ensure that the competent authorities apply less intrusive investigation methods if such methods enable a terrorist offence to be detected, prevented or prosecuted with adequate effectiveness. Decision-making authority should be structured so that the greater the invasion of privacy, the higher the level of authorization needed.

61. Adherence to international standards for privacy and human rights protection must be a tenet national law. Accordingly, a comprehensive data protection and privacy law is necessary to ensure that there are clear legal protections for individuals to prevent the excessive collection of personal information, that ensures measures are in place to ensure the accuracy of information, that creates limits on the use, storage, and sharing of the information, and which mandates that individuals are notified of how their information is used and that they have a right to access and redress, regardless of nationality and jurisdiction.

62. Strong independent oversight mandates must be established to review policies and practices, in order to ensure that there is strong oversight of the use of intrusive surveillance techniques and the processing of personal information. Therefore, there must be no secret surveillance system that is not under the review of an effective oversight body and all interferences must be authorized through an independent body.

63. All current and proposed counter-terrorism policies must include privacy impact assessments to review and communicate how the policy and technologies ensure that privacy risks are mitigated and privacy is considered at the earliest stages of policymaking.

64. The Special Rapporteur recommends that stronger safeguards be developed to ensure that the sharing of information between governments continues to protect the privacy of individuals.

65. The Special Rapporteur also recommends that stronger regulations are developed to limit Government access to information held by third parties, including reporting schemes, and to minimize the burden placed on third parties to collect additional information, and that constitutional and legal safeguards apply when third parties are acting on behalf of the State.

66. The Special Rapporteur warns that legislative language should be reconsidered to prevent the use of anti-terrorism powers for other purposes. New systems must be designed with a limitation of scope in the specifications.

For Governments

67. The Special Rapporteur urges Governments to articulate in detail how their surveillance policies uphold the principles of proportionality and necessity, in accordance with international human rights standards, and what measures have been taken to ensure against abuse.

68. The Special Rapporteur recommends open discussion and regular reporting on information-based surveillance programmes. Reports to legislative and oversight

A/HRC/13/37

bodies, as well as independent reviews of practices will help inform future policymaking and deliberation on anti-terrorism policy.

69. Any watch list- or profile-based surveillance programme must include due process safeguards for all individuals, including rights to redress. The principle of transparency must be upheld so that individuals can be informed as to why and how they were added to watch lists or how their profile was developed, and of the mechanisms for appeal without undue burdens.

70. Given the inherent dangers of data mining, the Special Rapporteur recommends that any information-based counter-terrorism programme should be subjected to robust and independent oversight. The Special Rapporteur also recommends against the development and use of data-mining techniques for counter-terrorism purposes.

71. In light of the risk of abuse of surveillance technologies, the Special Rapporteur recommends that equal amounts of research and development resources be devoted to privacy-enhancing technologies.

For the Human Rights Council

72. The Special Rapporteur recommends the development of a programme for global capacity-building on privacy protection. The international replication of anti-terrorism laws and the global standards on surveillance must be counterbalanced with greater awareness of the necessary safeguards for the protection of individuals' dignity.

73. The Special Rapporteur urges the Human Rights Council to establish a process that builds on existing principles of data protection to recommend measures for the creation of a global declaration on data protection and data privacy.

For the Human Rights Committee

74. The Special Rapporteur recommends that the Human Rights Committee begins drafting a new general comment on article 17 of the International Covenant on Civil and Political Rights, with the goal of elaborating a proper limitation test, thereby providing guidance to States on appropriate safeguards. The general comment should also give due attention to data protection as an attribute of the right to privacy, as enshrined in article 17 of the Covenant.

Exhibit JJ



THE PERMANENT REPRESENTATIVE
OF THE
UNITED STATES OF AMERICA
TO THE
UNITED NATIONS AND OTHER INTERNATIONAL ORGANIZATIONS
IN GENEVA

OHCHR REGISTRY

February 26, 2015

27 FEB 2015

Recipients SPD

David Kaye
Special Rapporteur on the Promotion of the Right to Freedom of Opinion and Expression
Office of the United Nations High Commissioner for Human Rights
Geneva, Switzerland

Dear Mr. Kaye:

The United States is pleased to respond to this first call for information from the new Special Rapporteur for the promotion and protection of the freedom of expression and opinion and looks forward to working with the Special Rapporteur during his occupancy of the mandate.

The United States has a long and proud tradition of defending freedom of expression, which is enshrined in our Constitution and robustly protected under our laws. Consistent with Article 19 of the International Covenant on Civil and Political Rights, these protections apply regardless of how the speech is articulated or the medium that is used.

In the United States, there are no laws that prohibit the development or use of encryption or anonymity online. Moreover, the United States Government strongly supports an open, interoperable, secure, and reliable Internet, and has long worked to promote accessibility, security, privacy, and freedom of expression online. Together with other States, the United States has worked to establish an international consensus around the principle that the same rights that people have offline must also be protected online, in particular freedom of expression.

As President Obama recently made clear, the United States firmly supports the development and robust adoption of strong encryption, which is a key tool to secure commerce and trade, safeguard private information, promote freedoms of expression and association, and strengthen cybersecurity. Encryption, as well as tools that assist with anonymity, are especially important in sensitive contexts where attribution could have negative political, social or personal consequences or when the privacy interests in the information are strong. In general, the free flow of information, opinions, and data helps foster transparency, creativity, innovation, and learning, and tools and methods that support this flow generate positive economic, social, and political consequences.

At the same time, terrorists and other criminals use encryption and anonymity tools to conceal and enable their crimes. This poses serious challenges for public safety. Society has an undeniable interest in law enforcement being able to investigate and prosecute terrorists and other criminals, and as President Obama recently made clear it is important to have a public



debate about how to address this issue. Misuse by a few, however, does not change the fact that responsibly deployed encryption helps secure many aspects of our daily lives, including our private communications and commerce. The United States will work to ensure that malicious actors can be held to account without weakening our commitment to strong encryption.

As a matter of policy, and consistent with our international commitments as a Participating State of the Wassenaar Arrangement, we continue to regulate the exports of certain forms of encryption. These items are controlled due to U.S. national security, foreign policy and law enforcement interests. The U.S. implementation of these controls can be found in the Export Administration Regulations, mainly in Sections 774 (the control list), and Sections 742.15 and 740.17 (licensing policy and license exceptions).

Consistent with this legal framework, as a matter of policy, the United States has long supported the development and use of strong encryption and anonymity-enabling tools online. The United States has a proud history of working with the international cryptographic community to develop and vet the strongest possible encryption algorithms for public and private sector stakeholders. This work dates back to the 1970s with international competitions that resulted in the Data Encryption Standard and, more recently, with the Advanced Encryption Standard, both of which became widely used international encryption standards. Currently, the Secure Hash Encryption (SHA-3), which was developed through another international competition we held, is in the process of becoming an international standard.

In addition, as part of the United States' commitment to defend and promote human rights online, the United States Government has provided funding to support the development and dissemination of anti-censorship and secure communications technologies to ensure that human rights defenders and vulnerable civil society communities, such as journalists, LGBT activists, and religious minorities, operating in repressive contexts are able to communicate securely, associate safely, and express themselves freely online.

Sincerely,



Pamela K. Hamamoto
Ambassador

Exhibit KK

United Nations

A/RES/69/166



General Assembly

Distr.: General
10 February 2015

Sixty-ninth session
Agenda item 68 (b)

Resolution adopted by the General Assembly on 18 December 2014

[on the report of the Third Committee (A/69/488/Add.2 and Corr.1)]

69/166. The right to privacy in the digital age

The General Assembly,

Reaffirming the purposes and principles of the Charter of the United Nations,

Reaffirming also the human rights and fundamental freedoms enshrined in the Universal Declaration of Human Rights¹ and relevant international human rights treaties, including the International Covenant on Civil and Political Rights² and the International Covenant on Economic, Social and Cultural Rights,²

Reaffirming further the Vienna Declaration and Programme of Action,³

Recalling its resolution 68/167 of 18 December 2013 on the right to privacy in the digital age,

Welcoming the adoption by the Human Rights Council of resolution 26/13 of 26 June 2014 on the promotion, protection and enjoyment of human rights on the Internet,⁴

Welcoming also the work of the Office of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, noting with interest its report on the subject,⁵ and recalling the panel discussion on the right to privacy in the digital age held during the twenty-seventh session of the Human Rights Council,

Noting the report of the Special Rapporteur of the Human Rights Council on the promotion and protection of human rights and fundamental freedoms while countering terrorism⁶ and the report of the Special Rapporteur of the Council on the promotion and protection of the right to freedom of opinion and expression,⁷

¹ Resolution 217 A (III).

² See resolution 2200 A (XXI), annex.

³ A/CONF.157/24 (Part I), chap. III.

⁴ See *Official Records of the General Assembly, Sixty-ninth Session, Supplement No. 53 (A/69/53)*, chap. V, sect. A.

⁵ A/HRC/27/37.

⁶ A/69/397.

⁷ A/HRC/23/40 and Corr.1.

14-67635 (E)



Please recycle 



Noting with appreciation general comment No. 16 of the Human Rights Committee on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation, while also noting the vast technological leaps that have taken place since its adoption,⁸

Recognizing the need to further discuss and analyse, based on international human rights law, issues relating to the promotion and protection of the right to privacy in the digital age, procedural safeguards, effective domestic oversight and remedies, the impact of surveillance on the right to privacy and other human rights, as well as the need to examine the principles of non-arbitrariness and lawfulness, and the relevance of necessity and proportionality assessments in relation to surveillance practices,

Noting the holding of the Global Multi-stakeholder Meeting on the Future of Internet Governance, "NETmundial", in São Paulo, Brazil, in April 2014, and recognizing that effectively addressing the challenges relating to the right to privacy in the context of modern communications technology will require an ongoing, concerted multi-stakeholder engagement,

Noting also that the rapid pace of technological development enables individuals all over the world to use new information and communication technologies and at the same time enhances the capacity of governments, companies and individuals to undertake surveillance, interception and data collection, which may violate or abuse human rights, in particular the right to privacy, as set out in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, and is therefore an issue of increasing concern,

Reaffirming the human right to privacy, according to which no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, and the right to the protection of the law against such interference, and recognizing that the exercise of the right to privacy is important for the realization of the right to freedom of expression and to hold opinions without interference and the right to freedom of peaceful assembly and association, and is one of the foundations of a democratic society,

Stressing the importance of full respect for the freedom to seek, receive and impart information, including the fundamental importance of access to information and democratic participation,

Noting that while metadata can provide benefits, certain types of metadata, when aggregated, can reveal personal information and can give an insight into an individual's behaviour, social relationships, private preferences and identity,

Emphasizing that unlawful or arbitrary surveillance and/or interception of communications, as well as unlawful or arbitrary collection of personal data, as highly intrusive acts, violate the right to privacy, can interfere with the right to freedom of expression and may contradict the tenets of a democratic society, including when undertaken on a mass scale,

Noting in particular that surveillance of digital communications must be consistent with international human rights obligations and must be conducted on the basis of a legal framework, which must be publicly accessible, clear, precise,

⁸ Official Records of the General Assembly, Forty-third Session, Supplement No. 40 (A/43/40), annex VI.

comprehensive and non-discriminatory and that any interference with the right to privacy must not be arbitrary or unlawful, bearing in mind what is reasonable to the pursuance of legitimate aims, and recalling that States that are parties to the International Covenant on Civil and Political Rights must undertake the necessary steps to adopt laws or other measures as may be necessary to give effect to the rights recognized in the Covenant,

Emphasizing that States must respect international human rights obligations regarding the right to privacy when they intercept digital communications of individuals and/or collect personal data and when they require disclosure of personal data from third parties, including private companies,

Recalling that business enterprises have a responsibility to respect human rights as set out in the Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework,⁹

Deeply concerned at the negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights,

Noting with deep concern that, in many countries, persons and organizations engaged in promoting and defending human rights and fundamental freedoms frequently face threats and harassment and suffer insecurity as well as unlawful or arbitrary interference with their right to privacy as a result of their activities,

Noting that while concerns about public security may justify the gathering and protection of certain sensitive information, States must ensure full compliance with their obligations under international human rights law,

Noting also in that respect that the prevention and suppression of terrorism is a public interest of great importance, while reaffirming that States must ensure that any measures taken to combat terrorism are in compliance with their obligations under international law, in particular international human rights, refugee and humanitarian law,

1. *Reaffirms* the right to privacy, according to which no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, and the right to the protection of the law against such interference, as set out in article 12 of the Universal Declaration of Human Rights¹ and article 17 of the International Covenant on Civil and Political Rights;²

2. *Recognizes* the global and open nature of the Internet and the rapid advancement in information and communications technologies as a driving force in accelerating progress towards development in its various forms;

3. *Affirms* that the same rights that people have offline must also be protected online, including the right to privacy;

4. *Calls upon* all States:

(a) To respect and protect the right to privacy, including in the context of digital communication;

⁹ A/HRC/17/31, annex.

(b) To take measures to put an end to violations of those rights and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law;

(c) To review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;

(d) To establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data;

(e) To provide individuals whose right to privacy has been violated by unlawful or arbitrary surveillance with access to an effective remedy, consistent with international human rights obligations;

5. *Encourages* the Human Rights Council to remain actively seized of the debate, with the purpose of identifying and clarifying principles, standards and best practices regarding the promotion and protection of the right to privacy, and to consider the possibility of establishing a special procedure to that end;

6. *Decides* to remain seized of the matter.

*73rd plenary meeting
18 December 2014*

Exhibit LL

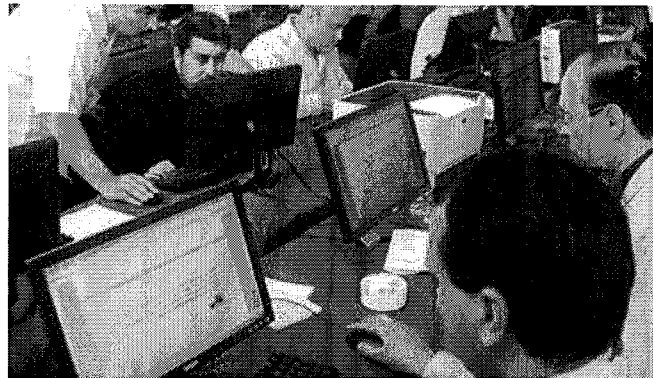


<https://cpj.org/x/4db4>

BLOG | SECURITY, SYRIA

Don't get your sources in Syria killed

By Eva Galperin/CPJ Guest Blogger



Journalists covering the Syrian uprising have been targeted with government surveillance, hacking, and malware. (AP/Bassem Tellawi)

Because foreign journalists have been virtually banned from Syria during the uprising against Bashar al-Assad's regime, news coverage has relied heavily on citizen journalists and international reporters working with sources inside the country. Syrians who communicate with foreign news media run the risk of being threatened, detained, tortured, or even killed.

This month, a Syrian court sentenced citizen journalist Mohammed Abdel Mawla al-Hariri to death for the crime of "high treason and contacts with foreign parties." He was arrested in April immediately after giving an interview with Al-Jazeera about conditions in his hometown of Daraa, in the southern part of the country. According to a report by the Skeyes Center for Media and Cultural Freedom, al-Hariri was tortured after his arrest. In the wake of the verdict and sentencing, he was transferred to Saidnaya military prison north of Damascus.

Al-Hariri is not alone. Press freedom groups such as CPJ and Reporters Without Borders have documented the detention of dozens of journalists; Syrian reporters, bloggers, and activists are regularly followed, arrested, and tortured.

Ordinary citizens who come into contact with international journalists are also targeted. Last fall, British journalist and filmmaker Sean McAllister met with a 25-year-old dissident and computer expert in Damascus who goes by the pseudonym "Kardokh." *Columbia Journalism Review* reports that Kardokh had agreed to be interviewed on camera, with the understanding that McAllister would blur his face before publishing the footage. But in October 2011, Syrian security agents arrested McAllister, seizing his laptop, cell phone, camera, and the footage for his documentary--including images and contact information that could be used to identify the activists he interviewed. When Kardokh heard that McAllister had been arrested, he immediately packed his bags and fled to Lebanon. Kardokh reports that several of the activists he had put in touch with McAllister had been arrested and at least one had disappeared. Channel 4, McAllister's news outlet, told *CJR* that the journalist had taken steps to protect his material but Syria proved unusually difficult.

The al-Assad regime's surveillance of telecommunications--cell phones, text messages, email, and Internet traffic--is remarkably extensive. Using equipment built in the West by companies such as BlueCoat, the Syrian government censors the Internet, blocks websites, and snoops on traffic using Deep Packet Inspection (DPI). As if that was not enough, the Syrian government has sought to expand its surveillance capabilities. Late last year, Bloomberg News reported that the Italian company Area SpA was seeking to pull out of a contract to build an Internet surveillance system in Syria that would give the government the power to "intercept, scan, and catalog virtually every email that flows through the country." The report went on to say that all work on the system had been suspended, but the scope of the project gives a glimpse into the regime's Orwellian vision.

In addition to its surveillance apparatus, the Syrian government may also benefit from intelligence gathered by pro-Syrian government hackers, who package malware that can capture webcam activity, disable the notification setting for certain antivirus programs, record key strokes, and steal passwords. The malware is specifically targeted at Syrian activists, including journalists and their sources, and spread through websites offering fake software downloads, fake PDFs purporting to relate to the formation of a new government after the revolution, links sent through email, Skype, and Facebook messages, and links left in the comment section of Facebook pages and YouTube videos that support the uprising.

In light of this exceptionally tricky landscape, here are some suggested best practices for international journalists communicating with sources and journalists inside of Syria.

Check for malware on your computer and have your sources check for malware on theirs. All of the security precautions in the world are useless if the Syrian government has keylogger files full of your passwords and full access to your most sensitive communications. This blog post describes how

to detect and remove DarkComet RAT, the most common Trojan installed by pro-Syrian government malware, which is not detectable by most antivirus scans.

Beware of fake websites, strange downloads, and suspicious links. Pro-Syrian government hackers have used fake Facebook and YouTube websites to covertly install malware and gather login credentials. Always check the URL bar at the top of your browser when you are entering your login credentials to make sure you are not visiting a fake website. Be cautious about downloading documents or software over the Internet, even if it is purportedly coming from a friend.

Beware of phones. Do not communicate over landlines or cell phones. Do not send text messages. If your source is concerned about giving away their location, they should refrain from using satellite phones as well.

Always use encryption. Do not use Skype. Skype purports to provide encrypted video chat, but a number of security weaknesses make it inadvisable for use when lives are at stake. If you are using a Web-based mail client, make sure that you are connecting using https--it helps to install the HTTPS Everywhere browser extension. Use PGP encryption for email. Use Adium and OTR (Off the Record) for encrypted messaging.

Syrian sources may be tempted to engage in insufficient security practices if they do not fully understand the regime's surveillance capabilities. It's incumbent on journalists to insist on secure communications when dealing with this exceptionally high-risk population. It's important to get the story out, but it's even more important to keep your sources safe.

Eva Galperin is international freedom of expression coordinator for the Electronic Frontier Foundation.

Comments

Some suggestions: Consider using Linux rather than Windows. It's free to download and use. You can put it on a USB stick and do your web browsing from there. Ubuntu Linux is a popular choice. You have very little chance of being affected by viruses if you use it. You can try Google Hangouts instead of Skype for video conferencing, it is fully encrypted. Use Firefox with the NoScript addon and use the Tor browser bundle for anonymity.

Exhibit MM

This site uses cookies. By continuing to browse the site you are agreeing to our use of

BloombergBusiness

Torture in Bahrain Becomes Routine With Help From Nokia Siemens

Vernon Silver and Ben Elgin

Bloomberg Markets

August 22, 2011 — 11:01 PM BST



Abdul Ghani Al Khanjar, activist, spokesman for the government-banned Bahraini National Committee for Martyrs and Victims of Torture. Photo courtesy of Abdul Ghani Al Khanjar.

The interrogation of Abdul Ghani Al Khanjar followed a pattern.

First, Bahraini jailers armed with stiff rubber hoses beat the 39-year-old school administrator and human rights activist in a windowless room two stories below ground in the Persian Gulf kingdom's National Security Apparatus building. Then, they dragged him upstairs for questioning by a uniformed officer armed with another kind of weapon: transcripts of his text messages and details from personal mobile phone conversations, he says.

If he refused to sufficiently explain his communications, he was sent back for more beatings, says Al Khanjar, who was detained from August 2010 to February.

"It was amazing," he says of the messages they obtained. "How did they know about these?"

The answer: Computers loaded with Western-made surveillance software generated the transcripts wielded in the interrogations described by Al Khanjar and scores of other detainees whose similar treatment was tracked by rights activists, Bloomberg Markets magazine reports in its October issue.

The spy gear in Bahrain was sold by Siemens AG, and maintained by Nokia Siemens Networks and NSN's

divested unit, Trovicor GmbH, according to two people whose positions at the companies gave them direct knowledge of the installations. Both requested anonymity because they have signed nondisclosure agreements. The sale and maintenance contracts were also confirmed by Ben Roome, a Nokia Siemens spokesman based in Farnborough, England.

The Only Way

The only way officers could have obtained messages was through the interception program, says Ahmed Aldoseri, director of information and communications technologies at Bahrain's Telecommunications Regulatory Authority. While he won't disclose details about the program, he says, "If they have a transcript of an SMS message, it's because the security organ was monitoring the user at their monitoring center."

The use of the system for interrogation in Bahrain illustrates how Western-produced surveillance technology sold to one authoritarian government became an investigative tool of choice to gather information about political dissidents -- and silence them.

Companies are free to sell such equipment almost anywhere. For the most part, the U.S. and European countries lack export controls to deter the use of such systems for repression.

Dangerous Products

"The technology is becoming very sophisticated, and the only thing limiting it is how deeply governments want to snoop into lives," says Rob Faris, research director of the Berkman Center for Internet and Society at Harvard University in Cambridge, Massachusetts. "Surveillance is typically a state secret, and we only get bits and pieces that leak out."

Some industry insiders now say their own products have become dangerous in the hands of regimes where law enforcement crosses the line to repression.

The images of the Arab spring crackdowns earlier this year unnerved Nikhil Gyamlani, who as a consultant for Trovicor and Nokia Siemens had developed monitoring systems and sold them to some of the countries. The authorities jammed or restricted communications to stymie gatherings and knew where to send riot police before a protest could even start, according to eyewitness reports.

For that to happen, government officials had to have some means of figuring out where to go or whom to target to nip protests in the bud, Gyamlani, 34, says.

Targeting With Technology

"There's very little chance a government is smart enough without this technology," he says while smoking Marlboros and drinking Bavarian beer on the patio of a pasta restaurant in Munich. Gyamlani says nondisclosure agreements with his former employers prohibit him from revealing details about specific countries he worked

with.

At least 30 people have been killed so far in this year's uprising in Bahrain, a U.S. ally situated between Qatar and Saudi Arabia that is home to the U.S. Navy's Fifth Fleet. Security forces beat paramedics, doctors and nurses who treated the wounded, and prosecutors have charged dozens of medical workers with crimes such as "incitement against the regime," according to Human Rights Watch. In June, the U.S. put Bahrain on its list of human rights violators.

A Secretive World

Across the Middle East in recent years, sales teams at Siemens, Nokia Siemens, Munich-based Trovicor and other companies have worked their connections among spy masters, police chiefs and military officers to provide country after country with monitoring gear, industry executives say. Their story is a window into a secretive world of surveillance businesses that is transforming the political and social fabric of countries from North Africa to the Persian Gulf.

Monitoring centers, as the systems are called, are sold around the globe by these companies and their competitors, such as Israel-based Nice Systems Ltd., and Verint Systems Inc., headquartered in Melville, New York. They form the heart of so-called lawful interception surveillance systems. The equipment is marketed largely to law enforcement agencies tracking terrorists and other criminals.

The toolbox allows more than the interception of phone calls, e-mails, text messages and Voice Over Internet Protocol calls such as those made using Skype. Some products can also secretly activate laptop webcams or microphones on mobile devices. They can change the contents of written communications in mid-transmission, use voice recognition to scan phone networks, and pinpoint people's locations through their mobile phones. The monitoring systems can scan communications for key words or recognize voices and then feed the data and recordings to operators at government agencies.

'Effective As Weapons'

Monitoring technology is among the newest artillery in an unfolding digital arms race, says Marietje Schaake, a European Parliament member who tracks abuses of information and communications technology. "We have to acknowledge that certain software products now are actually as effective as weapons," she says.

Uprisings from Tunisia to Bahrain have drawn strength from technologies such as social-networking sites and mobile-phone videos. Yet, the flip side of the technology that played a part in this year's "Facebook revolutions" may be far more forceful.

Rulers fought back, exploiting their citizens' digital connections with increasingly intrusive tools.

They've tapped a market that's worth more than \$3 billion a year, according to Jerry Lucas, president of McLean, Virginia-based TeleStrategies Inc., organizer of the ISS World trade shows for intelligence and lawful

interception businesses. He derives that estimate by applying per-employee revenue figures from publicly traded Verint's lawful intercept business across the mostly privately held industry.

'Push-Button Autocracy'

In the hands of autocrats, the surveillance gear is providing unprecedented power to monitor and crush dissent -- a phenomenon that Ben Wagner of the European University Institute in Florence, Italy, calls "push-button autocracy."

The technology has become pervasive. By the end of 2007, the Nokia Siemens Intelligence Solutions unit had more than 90 systems installed in 60 countries, according to company brochures.

Besides Bahrain, several other Middle Eastern nations that cracked down on uprisings this year -- including Egypt, Syria and Yemen -- also purchased monitoring centers from the chain of businesses now known as Trovicor. Trovicor equipment plays a surveillance role in at least 12 Middle Eastern and North African nations, according to the two people familiar with the installations.

Intelligence Solutions

Trovicor's precursor, which started in 1993 as the voice-and data-recording unit of Siemens, in 2007 became part of Nokia Siemens Networks, the world's second biggest maker of wireless communications equipment. NSN, a 50-50 joint venture with Espoo, Finland-based Nokia Oyj, sold the unit, known as Intelligence Solutions, in March 2009. The new owners, Guernsey-based Perusa Partners Fund 1 LP, renamed the business Trovicor, coined from the Latin and Esperanto words for find and heart, according to the company's website.

"We are very aware that communications technology can be used for good and ill," NSN spokesman Roome says. The elevated risk of human rights abuses was a major reason for NSN's exiting the monitoring-center business, and the company has since established a human rights policy and due diligence program, he says.

"Ultimately people who use this technology to infringe human rights are responsible for their actions," he says.

Little Documentation

Asked whether Trovicor or its predecessors sold monitoring centers to Middle Eastern nations that have cracked down on uprisings this year, Roome says the company can't talk about specific countries. NSN retained little documentation on the business after divesting it and has no data about the scope of its monitoring-center sales in the Mideast, he says.

Wolfram Trost, a spokesman for Munich-based Siemens, Europe's largest engineering company, says he can't comment because all documentation from the intelligence solutions unit had been transferred to Nokia Siemens.

Birgitt Fischer-Harrow, Trovicor's head of marketing communications, said Trovicor's contracts prevent it from disclosing its customers or the countries where it does business. She declined to comment further.

Trovicor's owners only invest in ethical businesses, says Christian Hollenberg, a founder of Munich-based Perusa GmbH, the adviser to the Perusa investment fund. He includes in that category Trovicor, which the fund owns in its entirety.

"It's a legal business, and it's part of every communications network in the civilized world," he says.

140 Allegations

Bahrain is confronting alleged human rights violations through the Bahrain Independent Commission of Inquiry, a panel established in June by royal decree to probe the recent violence, says government spokesman Abdul-Aziz bin Mubarak Al Khalifa, the international counselor at Bahrain's Information Affairs Authority. Since July 24, the commission has recorded 140 allegations of physical abuse and torture, according to an Aug. 10 statement on its website.

"The first things we're hearing is there wasn't systematic abuse or torture, but there were abuses by rogue individuals within the security apparatus," the government spokesman says. He says he isn't in a position to comment on surveillance equipment or a specific interrogation.

Valuable Tool

Most countries, including the U.S. and European Union member states, employ interception technology in their telecommunications and data systems. A valuable tool for law enforcement, monitoring technology typically is accompanied by strict privacy protections and meets standards established by the European Telecommunications Standards Institute and similar organizations. After 9/11, as part of the war on terror, the administration of President George W. Bush secretly -- and controversially -- authorized the National Security Agency to monitor communications to and from the U.S.

The Iranian Nobel Peace Prize winner Shirin Ebadi and other human rights activists have blamed Nokia Siemens for aiding government repression. In 2009, the company disclosed that it sold a monitoring center to Iran, prompting hearings in the European Parliament, proposals for tighter restrictions on U.S. trade with Iran, and an international "No to Nokia" boycott campaign.

While there have been credible reports the gear may have been used to crack down on Iranian dissidents, those claims have never been substantiated, NSN spokesman Roome says.

In Bahrain, officials routinely use surveillance in the arrest and torture of political opponents, according to Nabeel Rajab, president of the Bahrain Center for Human Rights. He says he has evidence of this from former detainees, including Al Khanjar, and their lawyers and family members.

'Even Our Children'

During the recent crackdown, Rajab says, monitoring was pervasive.

“Everyone was interrogated based on telephone calls that were checked -- and not only us, the activists,” he says. “Even our children, our wives, our sisters are being monitored.”

At Bahrain’s telecommunications regulator, Aldoseri says monitoring technology is used only by order of legal authorities such as judges and prosecutors. A former fighter pilot, Aldoseri, 33, led the drafting of Bahrain’s 2009 regulations for lawful interception.

Available online, the regulations make clear that every phone and Internet operator must provide the state with the ability to monitor communications. Phone companies also must track the location of phones within a 164-foot (50-meter) radius, the rules say.

‘Risk of Abuse’

“You have the risk of abuse, so we made it as public as possible,” Aldoseri says.

For Bahraini security agents, monitoring centers are essential for gathering and printing text messages and other transmissions, Aldoseri says.

He says it’s impossible to know which contractor’s monitoring center processed a particular text message transcript. He says he’s barred from identifying vendors.

“I can neither confirm nor deny that Trovicor is there,” he says. “It could be their monitoring center or it could be someone else.”

During the Arab spring, it was easy to spot the company’s fingerprints, says Gyamlani. Tuning in to Germany’s N24 news channel at his home in Munich, he immediately suspected that governments were abusing systems he’d installed.

Failed uprisings stood out to him because of the way the authorities quashed unrest before it spread, says Gyamlani, a native of India who moved to Germany 12 years ago to study and work.

Remote Kill Switches

Once the equipment is installed, Gyamlani says, there is no way to shut it down long distance. He’s forming a new company, GlassCube, that he says will feature remote kill switches as well as other technology and contract requirements that would enable companies to curb such abuses from afar.

“With the power comes a big responsibility; this is a business where people can get killed,” he says. “It was depressing to see there was no control mechanism.”

Visitors to Trovicor’s headquarters on the third floor of a glass office building in Munich are greeted by a life-size statue of the company’s mascot -- a stalking panther -- by the reception desk. The mascot is a carryover from the Nokia Siemens unit, as were most of the company’s roughly 170 workers, current and former employees say.

Former and current Trovicor and Nokia Siemens employees interviewed declined to be identified by name when discussing company business in specific countries. Clients contacted declined to speak on the record about specific contracts.

'Hidden Somewhere'

Al Khanjar, the Bahraini activist beaten during interrogations about his text messages, is in hiding today. He says he's reluctant to communicate by mobile phone and takes calls using Skype on a computer with software that disguises its location. The Internet connection is his only way of communicating with his wife and 9-year-old son.

"I'm hidden somewhere," he says. "I'm unfortunately in Bahrain. They're going to kill me. What to do? What to do?"

Al Khanjar took up the anti-torture cause after being detained and interrogated for six days in 2000. His jailers handcuffed him, hung him from a stick "like a goat" and beat the soles of his feet, he says.

He's now spokesman for the government-banned Bahraini National Committee for Martyrs and Victims of Torture. He and other activists have documented the security service's human rights violations for a decade, he says. His activism includes work with the United Nations Committee Against Torture and appearances on Qatar's Al Jazeera channel.

An Agonizing Stretch

Al Khanjar says that on Aug. 15, 2010, three days after he returned from speaking about human rights to a committee at the House of Lords in London, plainclothes police knocked on his door in Bahrain at about 2:30 a.m. It was the start of a six-month ordeal.

For his first 85 days or so in custody, Al Khanjar saw no one from the outside, he says. For one agonizing stretch, his jailers forced him to stand without sleeping for five days. At other times they beat him with hoses and their hands and threatened him with sexual abuse, he says.

Al Khanjar's interrogators repeatedly quizzed him about his contacts with Iran, where his wife's family originated generations ago, he says. They also focused on his activities in opposition politics and in religious gatherings with fellow Shiite Muslims, who form a majority of the kingdom's population yet are ruled by the Sunni minority.

Tracking Calls

"They had collected their information from tracking calls," he says, including whom he spoke with and what they said. "They told me a lot of things about our activities in the human rights field and political activities I'd participated in."

And they showed him several pages of transcripts of his text messages. An interrogator held the papers in front of Al Khanjar, pointing out the Arabic words printed in black ink on white paper and reading aloud details such as the dates and recipients of the texts, he says.

Al Khanjar says he sent one of the messages on June 9, 2009, after a flight to Qatar to visit a friend. His trip was thwarted when Qatar refused him entry at the Bahrain government's request. He suspected that his appearances on the satellite news channel, based in Qatar, explained the Bahraini government's interest in his travel there. Al Khanjar fired off the text to a fellow activist. "What happened to me is because of Al Jazeera," it read.

'No Windows'

More than a year later, when Al Khanjar was in jail, authorities seized on a transcript of that message, asking what he meant by it, particularly the reference to Al Jazeera, he says. Suspicious of his explanation, officers threatened to put him in a solitary confinement cell with no toilet two floors down -- the same floor where they tortured prisoners.

"You cannot hear anything," Al Khanjar says. "You don't know the time. You don't know if it's day or night. No windows."

Only after overhearing officers refer in radio chatter among themselves to their national security building as Jazeera did he conclude their interest in his innocuous text message was a misunderstanding that he had been making a reference to their facilities.

"They thought that I knew something about their code," he says.

A prosecutor charged Al Khanjar with crimes that included establishing a group in violation of the law and inciting and participating in unauthorized meetings of more than five people for the purpose of undermining national security, according to a copy of the indictment translated by the Bar Human Rights Committee of England and Wales.

Torture Testimony

An arm of the England and Wales lawyers association, the committee sent a delegation to Bahrain that observed an Oct. 28, 2010, hearing in the case against Al Khanjar and 22 others arrested at the same time.

The detainees testified about being tortured while in custody, according to the bar committee's February 2011 report: beatings, particularly to the legs and ears; being kept in stress positions or naked for prolonged periods; hanging in a position called falaqa in which the detainee is suspended from a bar and the soles of his feet beaten; and, in some cases, sexual abuse.

The actions violated both international law and the laws of Bahrain, the report concluded. "Credible and pervasive allegations of mistreatment and torture, which are dismissed as fabrication by the Public Prosecutor,

completely undermine the rule of law," it stated.

Convicted in Absentia

In February, before Al Khanjar's trial had reached its conclusion, protests flared and the government released all 23 detainees to relieve political tensions. Al Khanjar immediately went into hiding.

A separate military tribunal later tried him and others -- many, like him, in absentia -- and convicted them on charges that included trying to overthrow the government. Al Khanjar, who denies the charges in this and the earlier case, was sentenced to 15 years in prison.

Al Khanjar says the first of his communications used in the interrogations was intercepted in June 2009. At that time, the Nokia Siemens family of related companies was the only known supplier and maintainer of monitoring centers to Bahrain, the two people familiar with the installations say. The clusters of computers required constant upgrades by the companies, they say.

Company executives understood that they had the only monitoring-center computers in the country, based on conversations with Bahraini officials, one of those familiar with the situation says. The other says he knew of the arrangement from internal company communications. Neither knows whether the equipment originally installed and maintained by the companies is still in use.

Exclusive Provider

NSN and Trovicor's status as exclusive provider in Bahrain continued at least through 2009, the two people familiar with the installation say. That period of more than two years coincides with the dates of text messages used to interrogate scores of political detainees, human rights advocate Rajab says.

Based on his conversations with former detainees and their representatives, he says that authorities used messages that dated as far back as the mid-2000s, even in recent interrogations.

Schaake, 32, who represents the Netherlands in the European Parliament, says companies should be barred from exporting such equipment to countries with poor human rights records. U.S. and EU export laws and UN sanctions control just a narrow slice of technology such as weapons systems or data encryption. International embargoes that cover a broader range of equipment target only a small circle of the worst actors, such as Myanmar and North Korea.

Transparency and Accountability

"It is time for more pressure, for more transparency and accountability when it comes to these products and services," Schaake says. As a first step, Schaake says surveillance systems involving information and communications technology should join military items such as missile parts on lists of restricted exports.

Schaake helped to sponsor a parliamentary resolution in February 2010 that called for the EU's executive body,

the European Commission, to ban exports of such technology to regimes that could abuse it. The commission hasn't implemented the nonbinding resolution.

The U.S. Congress passed a law in 2010 barring federal contracts with any businesses that sold monitoring gear to Iran. An investigation ordered by Congress and completed in June by the Government Accountability Office was unable to identify any companies supplying the technology to Iran, partly because the business is so secretive, the agency reported.

Lack of Oversight

Al Khanjar says lightly regulated sales of lawful interception technology expose an industry lacking appropriate oversight.

"The United Nations should put pressure on those companies that supply equipment to these tyrant regimes," he says.

Bahraini government regulator Aldoseri says the companies are all too happy to sell the equipment regardless of what happens once it's installed.

"If you provide someone with a knife, you expect them to use it responsibly," he says. That's not necessarily the case with surveillance companies, he says.

"They don't ask any of the operators or security organs what happens after. They provide equipment to filter and monitor and they don't care about due process."

Before it's here, it's on the Bloomberg Terminal.

• Bahrain • Siemens AG • Nokia OYJ • Human Rights • Mobile Phones • Middle East • Verint Systems Inc • Law Enforcement • Software • Qatar

Exhibit NN

This site uses cookies. By continuing to browse the site you are agreeing to our use of

BloombergBusiness

Iranian Police Seizing Dissidents Get Aid Of Western Companies

Ben Elgin, Vernon Silver and Alan Katz
October 31, 2011 — 12:01 AM GMT



Iranian authorities routinely use surveillance to round-up and interrogate political activists, according to accounts provided by victims and human rights groups. Photographer: STR/AFP/Getty Images

The Iranian officers who knocked out Saeid Pourheydar's four front teeth also enlightened the opposition journalist. Held in Evin Prison for weeks following his arrest early last year for protesting, he says, he learned that he was not only fighting the regime, but also companies that armed Tehran with technology to monitor dissidents like him.

Pourheydar, 30, says the power of this enemy became clear as intelligence officers brandished transcripts of his mobile phone calls, e-mails and text messages during his detention. About half the political prisoners he met in jail told him police had tracked their communications and movements through their cell phones, he says.

"This is a commerce of death for the companies that place this technology in the hands of dictatorships," Pourheydar says.

Even as the pariah state pursued a brutal political crackdown, including arrests and executions surrounding its contested 2009 elections, European companies supplied Iran with location tracking and text-message monitoring equipment that can turn mobile phones into tools for surveillance.

Stockholm-based Ericsson AB, Creativity Software Ltd. of the U.K. and Dublin-based AdaptiveMobile

Security Ltd. marketed or provided gear over the past two years that Iran's law enforcement or state security agencies would have access to, according to more than 100 documents and interviews with more than two dozen technicians and managers who worked on the systems.

Ericsson and Creativity Software offered technology expressly for law enforcement use -- including a location-monitoring product proposed by Ericsson in early 2009 and one sold this year by Creativity, according to the interviews.

Tracking Political Activists

The findings provide a rare window into how companies equip Iran's surveillance operation.

Iranian authorities routinely use surveillance to round-up and interrogate political activists, according to accounts provided by victims and human rights groups.

The suppliers of this gear are complicit in the human rights abuses for which Iran has been repeatedly condemned, U.S. Senator Mark Kirk says.

"The CEOs of these companies have no ability to look themselves in the mirror," says Kirk, an Illinois Republican who is sponsoring legislation to tighten sanctions against selling Iran tools for repression. "If they are making such sales, then probably a poor human rights activist is being hooked up to alligator clips because of what they've done."

'Little Distinction'

Whether the technology is destined for police, security services or other intelligence agencies makes little difference, says Mark Dubowitz, executive director of the Washington-based Foundation for Defense of Democracies, a policy group focusing on terrorism.

"There's very little distinction between the arms of the Iranian regime in terms of the use of technologies to monitor and target dissidents," he says.

Ericsson, the world's largest maker of wireless networks, confirmed that in the fourth quarter of 2009 it sold a mobile-positioning center for customer billing purposes to MTN Irancell Telecommunications Services Co., Iran's second-largest mobile provider.

When Iranian security officers needed to locate a target one night in late 2009, one former Ericsson employee says he got an emergency call to come into the office to fix a glitch in an Ericsson positioning center.

Ericsson says it will continue to maintain the system, but that it decided in October 2010 it would no longer sell any products into Iran due to recent efforts to tighten sanctions.

Enabling Law Enforcement

Early this year, Creativity Software sold a system that enables Iranian law enforcement and security forces to monitor cell phone locations, according to three people familiar with the transaction. With it, police can track a target's movements every 15 seconds and plot the locations on a map, according to a 19-page company product specification document. Creativity Software confirms that Irancell is a client, but declined to discuss sales of any location-tracking gear for law enforcement purposes, saying it would breach contract confidentiality.

AdaptiveMobile, backed by the investment arm of Intel Corp., proposed a system in partnership with Ericsson for Iran's largest mobile provider in 2010 that would filter, block and store cell phone text messages, according to two people familiar with the discussions. An Ericsson spokesman confirmed the proposal.

The Irish company still services commercial gear for a similar system it sold in 2008 to Irancell. Police have access to the system, say two former Irancell managers.

Calls for Controls

AdaptiveMobile says its technologies are for fighting spam, viruses and "inappropriate content," not designed or sold for law enforcement. It says it plans to cease doing business in Iran when its contract is up in late 2012, because continuing in Iran's current political climate could damage its reputation.

The three European companies continued to do business in Iran amid calls in the U.S. and European Union for greater export controls on such gear. It is legal in most countries to sell this technology to Iran.

And they continued after competitor Nokia Siemens Networks faced an international "No to Nokia" boycott and European parliamentary hearings after its 2008 delivery of communications intercept equipment to Iran.

Exports of these systems are largely unregulated, and industry secrecy can make sales difficult to document, says Dubowitz. The U.S. Government Accountability Office reported in June that it had been unable to identify any companies selling systems to Iran for monitoring or interfering with citizens' free speech.

Telling the World

Iran's electronic repression came of age after the country's June 2009 presidential elections, which sparked international allegations of vote-rigging when Mahmoud Ahmadinejad was declared the winner over three challengers.

In a precursor to this year's Arab Spring, citizens turned to digital communications such as text messages and social networking to organize demonstrations and tell the world what was happening as the government cracked down. Texting has become the predominant means of digital communications because more than 70 percent of Iranian households have a mobile phone -- four-times greater than the percentage with internet access.

While unrest has shaken or toppled other authoritarian regimes this year, sophisticated monitoring helped mute protests and activism in Iran, according to Mahmood Enayat, director of the Iran Media Program at the University of Pennsylvania. Iran is clearly employing technology to neutralize political opposition, he says.

Political Executions

Last year the government executed approximately 312 people, with more than three dozen killed for the charge of "Moharebeh," which includes political offenses, according to a U.S. State Department report. Hundreds of people have been convicted by Iranian courts for offenses related to election protests, according to New York-based nonprofit group Human Rights Watch.

The increased brutality is partly a result of the regime's stepped-up technology to identify and intimidate dissidents, says Eileen Chamberlain Donahoe, the U.S. Ambassador to the United Nations Human Rights Council.

"Their capacity for doing bad things has been enhanced by the use of technology," she says. "It has made it possible to really target people in ways that we've never seen before."

The Iranian Foreign Ministry did not respond to a faxed request for comment.

Phone as Enemy

Mansoureh Shojaee, a women's rights activist who fled to Germany after being arrested in December 2009 and jailed for a month, says she concluded that all her communications were under watch. When she planned to meet with fellow activists, police routinely called her or her contacts to say they knew where she was headed, she says.

Interrogators at Tehran's notorious Evin Prison asked Shojaee, 53, about her acquaintances and displayed call records and transcripts going back several months.

"My mobile phone was my enemy, my laptop was my enemy, my landline was my enemy," says Shojaee, who turned to using pay phones.

Iran is one of many authoritarian countries across the Mideast and North Africa employing Western surveillance tools for political repression. In Bahrain, for instance, communications monitoring centers sold by Siemens AG, and maintained by Espoo, Finland-based Nokia Siemens Networks and then its divested unit, Trovicor GmbH, have been used to track and arrest activists, according to a Bloomberg News investigation.

Corporate Regrets

After the backlash for its 2008 sale to Iran, NSN expressed regret and noted "credible reports" that the government had used communications technology to suppress dissent. Much of NSN's gear in Iran has since

been swapped out in favor of China's Huawei Technologies Co., according to Ben Roome, spokesman for NSN.

Huawei spokesman Ross Gan declined in an e-mail response to provide details "due to commercial sensitivities."

"Any equipment that we provide our customers is strictly for commercial use only and that applies to all of the markets in which we operate around the world," he said.

Most phone networks around the world are expected to contain law enforcement equipment in order to help track terrorists and criminals and handle emergencies.

A rapidly growing global business, the "lawful interception" and information intelligence market now generates more than \$3 billion in annual sales, according to Jerry Lucas, president of McLean, Virginia-based TeleStrategies Inc., which organizes industry trade shows worldwide.

'Evil Purposes'

Even when companies sell location and filtering tools for commercial purposes -- from billing and managing network traffic to fighting spam and offering location-based advertising -- they can be vulnerable to misuse by law enforcement.

"Companies can always come up with a legitimate sounding cover, but they will invariably find their products put to evil purposes," says Andrew Apostolou, senior program manager for Iran at Freedom House, a human rights group.

The Iranian government has asked the phone companies to equip themselves with improved tracking and text message storing and sorting technologies. For example, when government-controlled Mobile Communication Company of Iran sought a new system for handling text messages in early 2010, the operator, known as MCI, mandated that bidders also supply lawful interception technology capable of copying and storing text messages for later retrieval, according to a copy of the request.

Thousands Per Second

Ericsson, which bid on the system, was told by MCI, the country's largest wireless operator, to partner with AdaptiveMobile for monitoring and filtering technology, according to Ericsson spokesman Fredrik Hallstan. Ericsson didn't win the contract, he says.

The 3.9 million-euro (\$5.5 million) system AdaptiveMobile proposed could handle more than 10,000 messages per second and archive them for a period of 180 days, according to a company proposal. The archive would contain 54 terabytes of storage, according to the document. That's big enough for all the data gathered by the Hubble Space Telescope over 20 years.

NSN, which was in discussions with MCI about the project, flinched at this. The company had just come under fire for providing a monitoring center to Iran and was formulating new human rights policies. It decided against a formal bid because it worried about how the storage and monitoring features might be used, according to company spokesman Roome.

“Certain capabilities required of the system were not compatible with our human rights policy given the environment in Iran,” he says.

Ericsson’s Location System

Ericsson, the telecommunications giant with \$28 billion in sales last year, in 2008 supplied Irancell with its Mobile Positioning System 9.0 for locating subscribers -- a test system that Ericsson says Irancell didn’t buy and could use only on a limited scale.

Ericsson later sold Irancell the positioning-data component of the test system, says Richard Carter, Ericsson’s Istanbul-based head of commercial, sourcing and partnering in the Middle East and the country manager for Iran. It was sold in late 2009, the company confirmed. Known as a Serving Mobile Positioning Centre, the box calculates a person’s position and logs the data.

A former Irancell manager said that all such systems supplied to the mobile operator, including technology from Ericsson, were accessible by law enforcement agencies.

The former Ericsson employee urgently called in to fix the system in late 2009 says he was told that Iranian intelligence officers were attempting to pinpoint the location of someone in the Zahedan area of southeast Iran.

‘Deep Concern’

Before the election, on January 24, 2009, Ericsson officials pitched a tracking system specifically for Iran’s security agencies to MCI, according to a seven-page agenda and another document describing the Tehran meeting.

One month earlier, the U.N. General Assembly had expressed “deep concern at serious human rights violations” in Iran.

Law enforcement agents would be able to track subscribers with “easy and friendly” identification of geographic positions on a map, according to Ericsson’s 51-page proposal to MCI, which serves 44 million subscribers.

A list of basic features says maps could reveal the whereabouts of 200,000 MCI mobile-phone subscribers at a time and archive the locations for later analysis.

The system Ericsson proposed offered capabilities for law enforcement referred to as “PoLIS” that would allow

the interception of all phone calls occurring in a specific area, among other features, according to a copy of the proposal.

For State Security

Ericsson would have partnered with an Estonian software firm, Reach-U, whose tracking software “is designed for state security agencies,” according to one of the documents in the proposal.

Ericsson’s Carter says the discussions with MCI were preliminary and came to a halt as turmoil swept the country in 2009. He couldn’t find any reference to PoLIS features, he says.

Everything supplied by Ericsson to Iran complied with international trade embargoes, Carter says, adding that their products have been a positive force in the Middle East by promoting communications and commerce. “Ultimately, telecom is a force for good in society,” he says.

MCI did not respond to several requests for comment. Rich Mkhondo, corporate affairs executive for Johannesburg-based MTN Group, which owns 49 percent of Irancell and operates the network, declined to comment. Reach-U sales director Henry Aljand also declined to comment.

Ericsson Employee Tracked

Siavash Fahimi, an Ericsson employee, saw up close how these systems can be abused.

The 27-year-old Iranian worked for Ericsson in Tehran until 2010, installing several different systems.

Sipping tea last month beneath a tangerine tree outside a café in central Turkey, Fahimi recounts how he joined the protests that spilled into the streets in June 2009.

Police arrested him on the outskirts of a rally that December, beating him with fists and a baton and jailing him for 52 days. Security agents interrogated him 14 times, presenting transcripts of text messages plus an elaborate diagram showing all the people he’d called -- and then everyone they’d called.

Victim of Technology

They knew where he was at specific times, producing phone location records. And they pressed him to admit he was a spy, threatening to arrest his friends and family unless he supplied more information.

“It was a tool they used to put pressure on us,” he says. “They wanted us to confess.”

Fahimi, who fled to Turkey after receiving a two-year prison sentence for his role in the protests, can’t be sure that Ericsson technology aided his interrogators, but he is familiar with the capabilities of these types of systems.

“I worked on the technology and I was a victim of the technology, as well,” Fahimi says.

He has no problem with legitimate monitoring that has court authorization. That isn't the case in Iran, he says.

“They can monitor whoever they want, for their purposes, not for the benefit of society and people.”

Creativity Software, based southwest of London in Kingston upon Thames, announced a deal in August 2009 to sell Irancell commercial customer location services.

Early this year, it sold the mobile phone provider a second system that allows law enforcement to locate and track targets, according to three people familiar with the transaction.

Every 15 Seconds

The system can record a person's location every 15 seconds -- eight times more frequently than a similar system the company sold in Yemen, according to company documents. A tool called “geofences” triggers an alarm when two targets come in close proximity to each other. The system also stores the data and can generate reports of a person's movements. A former Creativity Software manager said the Iran system was far more sophisticated than any other systems the company had sold in the Middle East.

Creativity Software held initial conversations with MCI early this year to provide a nearly identical system, according to two former Creativity managers, though the status of those talks is unclear.

Employees at Creativity Software were concerned about selling the technology to Iran, says Venu Gokaram, who worked as a test manager for the company until early this year.

Worried Employees

“A lot of people were not happy they were working on a project in Iran,” he says. “They were worried about how the product was going to be used.”

Gokaram says he worked only on commercial products and didn't share those concerns. He declined to discuss specifics about any technology deployed in Iran.

Creativity Software, which is privately-held and partly funded by London-based venture capital firm MMC Ventures, announced last November that it had made four sales in six months in the Middle East for law enforcement purposes without identifying the mobile operator clients.

Saul Olivares, market development director at Creativity Software, declined to discuss sales of law enforcement technology, but in an e-mail he pointed to its practical benefits, such as locating individuals during disasters, for ambulance crews and in other emergencies.

Jon Coker, investment director at MMC Ventures and a board member at Creativity Software, declined to comment.

Texts as Threats

In addition to tracking people's whereabouts, the country also sought assistance to monitor the text messages zooming across its networks. Texting had become a threat to the regime, say rights groups.

In 2008, AdaptiveMobile sold Irancell technology to filter, block and store text messages. Text message monitoring was required by security forces, who use the technology for their own purposes, according to two former Irancell managers.

An Adaptive document detailed the system requirements. It would analyze all messages in English, Persian or Arabic for keywords or phrases; store them; and flag those caught by filters for review.

Law enforcement officials requested specific features, according to three people familiar with the discussions. One request was to be able to change the content of messages, said a former senior engineer at Irancell.

Two former Adaptive employees say there were discussions within the company about law enforcement requests as the project came together.

While Adaptive's executives confirm the Irancell deal and an upgrade to the system to handle more messages, they say it was intended only for commercial purposes. They deny any involvement with Iran security or police.

Law Enforcement Requests

"We are sure our product is not being used in this way," says AdaptiveMobile CEO Brian Collins.

He says a company search of internal records turned up one or two documents that contain references to law enforcement requests. The Irish company told Irancell that "under no circumstances was our technology to be used for law enforcement purposes," he says.

Collins says he believed that one of Bloomberg's sources was a former employee with an axe to grind, and that at least one of the documents in Bloomberg's possession had been doctored, without being more specific.

Asked if AdaptiveMobile's systems could scour for political content on activists, Chief Operating Officer Gareth Maclachlan said, "Technically, yes, it is possible." He says he doubted they would be practical for that purpose.

Changed Landscape

"The political landscape has changed quite a bit since 2007," Maclachlan says. "We're not going to chase any

more business there.”

As recently as 2010, AdaptiveMobile attempted to sell a similar product to MCI, the one on which it partnered with Ericsson. Collins and Maclachlan say they were not familiar with details of the proposal.

“This is business that was not pursued,” Collins said later in an e-mail.

Intel Capital, the investment arm of the world’s largest chipmaker, has invested 6 million euros in AdaptiveMobile, which was founded in 2003. Kristof Sehmke, an Intel Capital spokesman, said in a statement that his company strives to comply with all legal requirements.

“Intel will not invest in a company unless they agree to do the same,” he said.

Clamping Down

While many countries permit the sale of surveillance technology to Iran, regulators concerned about human rights abuses are beginning to clamp down.

The European Union took aim at Iran’s growing surveillance capabilities in October 2010, enacting new sanctions that include prohibitions for goods that can be used for “internal repression.” The regulations, however, focused mostly on low-tech items, such as vehicles equipped with water cannons and razor barbed wire.

In September, the European Parliament broadened its surveillance concerns beyond Iran, voting for a block on exports of systems if the purchasing country uses the gear “in connection with a violation of human rights.”

U.S. companies have been banned from virtually all trade with Iran since 1995, when President Bill Clinton declared it a threat to national security.

In July 2010, President Barack Obama signed into law new U.S. sanctions that bar federal agencies from doing business with companies that export to Iran any technology specifically used to disrupt, monitor or restrict the speech of Iranians.

‘Blood on Hands’

According to data compiled by Bloomberg, Ericsson signed at least 27 contracts worth \$5.25 million with the U.S. government from the start of 2009 to the end of 2010. The data showed no U.S. government business with AdaptiveMobile or Creativity Software.

“If a Western or outside interest ends up cooperating with Iranian authorities, then they come to the table with blood on their hands,” says Kirk, the U.S. senator.

After his arrest early last year, Pourheydar, the opposition journalist, says police accused him of speaking to foreign media such as BBC and Voice of America. Their evidence: unbroadcast mobile phone calls captured, recorded and transcribed, he says. They also had transcripts of his e-mails and text messages. He never learned which companies provided the technology that made it possible.

Mock Execution

The beatings that claimed four of his front teeth were nothing compared to the mental torture, he says. Guards one day announced he was to be executed. They forced him to stand on a stool, blindfolded and handcuffed, with a tightened noose around his neck. He remained there, legs trembling, for 25 minutes, until guards called it off and told him they'd be back. After being released to await a prison sentence from the court, Pourheydar fled to Turkey.

One evening last month, in a crowded restaurant in the Turkish city of Nigde, Pourheydar recounted his ordeal while nervously tapping a visitor's business card on the table and dabbing sweat from his neck and forehead.

"All these companies, which sell telecommunications services and listening devices to Iran, directly have roles in keeping this regime in power," he says.

Before it's here, it's on the Bloomberg Terminal.

• Iran • Ericsson AB • Mobile Phones • Law Enforcement • Creativity Software Ltd • Human Rights • European Parliament • Nokia OYJ • Siemens AG

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

PROOF OF SERVICE

I am a citizen of the United States of America and employed in London, the United Kingdom. I am over the age of 18 and not a party to the within action. My business address is Privacy International, 62 Britton Street, London EC1M 5UY, United Kingdom.

On March 3, 2016, I caused to be served through mail (FedEx) and/or e-mail on each person on the attached Service List the foregoing document described as:

DECLARATION OF CAROLINE WILSON PALOW IN SUPPORT OF BRIEF OF *AMICI CURIAE* PRIVACY INTERNATIONAL AND HUMAN RIGHTS WATCH and EXHIBITS

Service List

Service Type	Counsel Served	Party
E-mail*	Theodore J. Boutrous, Jr. Nicola T. Hanna Eric D. Vandavelde Gibson, Dunn & Crutcher LLP 333 South Grand Avenue Los Angeles, CA 90071-3197 Telephone: (213) 229-7000 Facsimile: (213) 229-7520 Email: tboutrous@gibsondunn.com nhanna@gibsondunn.com evandavelde@gibsondunn.com	Apple, Inc.
E-mail*	Theodore B. Olson Gibson, Dunn & Crutcher LLP 1050 Connecticut Avenue, N.W. Washington, D.C. 20036-5306 Telephone: (202) 955-8500 Facsimile: (202) 467-0539 Email: tolson@gibsondunn.com	Apple, Inc.

<p>1 E-mail*</p> <p>2</p> <p>3</p> <p>4</p> <p>5</p> <p>6</p> <p>7</p>	<p>Marc J. Zwillinger Jeffrey G. Landis Zwillgen PLLC 1900 M Street N.W., Suite 250 Washington, D.C. 20036 Telephone: (202) 706-5202 Facsimile: (202) 706-5298 Email: marc@zwillgen.com jeff@zwillgen.com</p>	<p>Apple, Inc.</p>
<p>8 Mail & E-mail</p> <p>9</p> <p>10</p> <p>11</p> <p>12</p> <p>13</p> <p>14</p>	<p>Eileen M. Decker Patricia A. Donahue Tracy L. Wilkison Allen W. Chui 1500 United States Courthouse 7312 North Spring Street Los Angeles, California 90012 Telephone: (213) 894-0622/2435 Facsimile: (213) 894-8601-7520 Email: Tracy.Wilkison@usdoj.gov Allen.Chiu@usdoj.gov</p>	<p>United States of America</p>

15 *Apple, Inc. has consented in writing to service by electronic means in accordance
 16 with Federal Rule of Civil Procedure 5(b)(E), Local Civil Rule 5-3.1.1, and Local
 17 Criminal Rule 49-1.3.2(b).

18


19 I declare under penalty of perjury under the laws of the United States of
 20 America that the foregoing is true and correct and that I have made service at the
 21 direction of a member of the bar of this Court.

22 Executed on March 3, 2016 in London, United Kingdom

23

24

25

26 

27 _____

28 Sara Nelson