THE HIGH COURT
COMMERCIAL

Record No: 2016/4809P

Between:

Data Protection Commissioner

Plaintiff

-and-

Facebook Ireland Limited and Maximillian Schrems

Defendants

AFFIDAVIT OF ALAN BUTLER, ELECTRONIC PRIVACY INFORMATION CENTER

I, Alan Butler, lawyer, of Electronic Privacy Information Center, 1718 Connecticut Avenue NW, Washington D.C., 20009, USA aged 18 years and upwards **MAKE OATH** and say as follows:

1. I am a U.S. qualified lawyer called to the District of Columbia Bar and Senior Legal Counsel with the Electronic Privacy Information Center (hereafter "EPIC"), an *amicus curiae* in the within proceedings.

2. I am duly authorized to make this Affidavit on behalf of EPIC for the purpose of assisting the High Court in Ireland in relation to electronic surveillance/data privacy law and practice in the U.S. I make this affidavit from facts within my own knowledge, save where otherwise appears, and, where so appearing, I believe same to be true and accurate.

INTRODUCTION

3. I believe that four aspects of U.S. law are relevant to the proceedings before the Irish High Court: first, the U.S. legal regime for protection of personal data processed by either private or public sector entities; second, current U.S. surveillance law as it applies to the collection of personal data of E.U. citizens; third, the specific remedies available to E.U. citizens whose personal data has been transferred to the U.S.; fourth, and finally, the legal obstacles to accessing that redress.

4. What follows is a brief synopsis of the operative legal framework for these key issues. I also use this affidavit to, where necessary, put relevant U.S. legislation and other legal materials, to which EPIC intends to refer in detailed legal submissions, before the Court. For ease of reference, I beg to refer to a tabbed booklet of copies of the said legislation and legal

materials upon which marked with the letters "**AB 1**" I have signed my named prior to the signing hereof.

I PROTECTION OF PERSONAL DATA IN THE UNITED STATES

5. There is no explicit right to privacy under the United States Constitution.[1]

a) Segmented Structure of U.S. Privacy and Data Protection Law

6. Privacy law in the U.S. is segmented both because constitutional privacy restrictions do not limit the actions of private companies and because statutory privacy protections have been adopted on a somewhat piecemeal, industry-specific basis. Additionally, the U.S. Supreme Court has to date declined to recognize a constitutional right to informational privacy. *See Nat'l Aeronautics and Space Admin. v. Nelson*, 562 U.S. 134 (2011).

7. The true position is that U.S. lacks a comprehensive privacy protection law for the private sector. Instead there is a patchwork of federal laws covering different categories of personal information.[2]

8. President Obama proposed the adoption of a Consumer Privacy Bill of Rights, a set of guiding principles for data privacy, at the beginning of his second term.[3] The U.S. Congress has not taken any steps to adopt such a framework.

9. There is no independent privacy oversight agency in the United States.[4] Instead, authority over data privacy has been divided between various agencies with different jurisdictions and powers, ranging from the Office of Management and Budget, which plays a role in setting policy for federal agencies under the Privacy Act, to the Department of Health and Human Services (enforcement of HIPPA), to the Federal Communications Commission (enforcement of privacy rules governing telephone providers, cable companies, and internet service providers).

10. The Federal Trade Commission (FTC) has broad enforcement authority over commercial actors, for instance in preventing "persons, partnerships, or corporations . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce" (15 U.S.C. § 45(a)(2)). Many of the largest online companies, including search engines, email services, and social network platforms, are regulated under the FTC's unfair and deceptive authority, but the Commission has no general authority to review surveillance activities.

---

[1] EPIC, PRIVACY AND HUMAN RIGHTS 1007 (2006) is at Tab 1 in the Booklet AB 1.
[2] *Id.*
[3] THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 11-22 (Feb 23, 2012).
[4] EPIC, *supra* note 1.

11. FTC enforcement actions therefore largely focused on whether companies honored their own privacy promises (an unfair or deceptive act or practice). The FTC does not have independent authority to punish or fine a violator, and can only seek a fine in court if its ruling is later violated (15 U.S.C. §§ 45(l)–(m)). Consumers whose privacy has been violated by unfair or deceptive trade practices do not have a private right of action under the FTC Act to obtain redress.

b) Definitions of "Personal Information"

12. While the E.U definition of personal data encompasses "any information relating to an identified or identifiable natural person" whether identified "directly or indirectly,"[5] U.S. conceptions of personal data and privacy, with few exceptions, tend to be limited to "instances where data refers to an **identified** individual" rather than to an identifiable individual.[6]

13. In the consumer privacy context, for instance, U.S. courts are currently split about whether static IP addresses and other unique device identifiers are covered by existing privacy law.[7] Similarly, the FTC decided not to adopt recommendations on to ensure de-identification of personal data is uniform and effective, considering de-identification a technical issue outside its purview.[8]

14. In the context of government surveillance, the definition of personal information is even narrower. The NSA minimization procedures, revised under PPD-28 to extend certain privacy protections to non-U.S. persons (see below), only prohibit the retention and dissemination of a narrowly defined category of personal information. Under the Defense Department intelligence manual, personal information is defined as:

> *Information that is reasonably likely to identify one or more specific U.S. persons. USPI may be either a single item of information or information that, when*

---

[5] Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; 1995 O.J. (L 281) 31, 38 [hereinafter Directive 95/46/EC];; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L119) 1, 33 [hereinafter Regulation 2016/679]..

[6] Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CALIF. L. REV. 877, 891 (2014) (emphasis added).

[7] *Compare YerShov v. Gannett Satellite Info. Network Inc.*, 820 F.3d 482, 485-86 (1st. Cir. 2016) (ruling that information the video viewed, device identifier, and device GPS coordinates were "personally identifiable information" (PII) under the Video Privacy Protection Act (VPPA)), *with In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 281–90 (3d Cir. 2016) (holding static IP addresses, even when combined with browser and unique device identifiers are not PII, under the VPPA).

[8] Electronic Privacy Information Center, Comments on In the Matter of Compete Inc. (Nov. 19, 2012) (advocating adoption of a best practices guide for de-identification); Federal Trade Commission, Letter Re: In the Matter of Compete, Inc., File No. 1023155, Docket No. C-4384 (Feb. 20, 2013), (declining to adopt such a guide, stating "company's responsibility to keep abreast of and select the technology that it believes best meets its needs and requirements").

combined with other information, is reasonably likely to identify one or more specific U.S. persons.

DODM 5240.01: PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES § G.2 (Aug. 8, 2016) [hereinafter DODM].

15. More generally, the United States does not view technological access, like electronic scanning, as implicating privacy or data protection concerns. The Director of National Intelligence (DNI) general counsel recently made this point clear in an article about the Fourth Amendment:

> *If the government electronically scans electronic communications, even the content of those communications, to identify those that it is lawfully entitled to collect, and no one ever sees a non-responsive communication, or even knows that it exists, where is the actual harm?*
>
> Robert S. Litt, *The Fourth Amendment in the Information Age,* 126 Yale. L. J. F. 8, 15 (2016).

II CURRENT U.S. SURVEILLANCE LAW

16. The laws and regulations governing access to personal data of E.U. citizens by the U.S. Intelligence Community (USIC) include the Fourth Amendment to the U.S. Constitution, the Foreign Intelligence Surveillance Act (FISA) (and, in particular, Section 702 thereof), the Electronic Communications Privacy Act (ECPA), and Executive Order 12333 (EO12333), Presidential Policy Directive 28 (PPD-28), and the United States Signals Intelligence Directive SP0018 (USSID 18).

a) The Fourth Amendment to the U.S. Constitution

17. The Fourth Amendment to the U.S. Constitution provides:

> *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*
>
> U.S. CONST. AMEND. IV.

18. The Fourth Amendment restricts "searches" and "seizures" carried out by Government officials. The Fourth Amendment does not restrict private actors. The U.S. Supreme Court has concluded:

> *The first clause of the Fourth Amendment provides that the 'right of the people to be secure in their persons, houses, papers and effects, against unreasonable*

searches and seizures, shall not be violated . . .'" This text protects two types of expectations, one involving 'searches,' the other 'seizures.' A 'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed. A 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property. This Court has also consistently construed ***this protection as proscribing only governmental action****; it is wholly inapplicable 'to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official.'*

United States v. Jacobsen, 466 U.S. 109, 113 (1984) (emphasis added).

19. The Supreme Court has limited the type of personal data protected under the Fourth Amendment. In *Smith v. Maryland*, the Court considered the use of a 'pen register' device to record telephone numbers dialed by a criminal suspect (but not the content of the calls) without a warrant. 442 U.S. 735 (1979). The Court held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties" such as telephone companies. *Id.* at 743–44. Accordingly, the mass collection of 'non content' personal data is not currently prohibited by the Fourth Amendment. The Court has not re-visited this issue for many years and has not decided upon the key issue of whether the Fourth Amendment protects the content of electronic communications such as e-mails and other messages held by third parties.

20. At least one U.S. Court of Appeals has, however, had the occasion to consider whether the Fourth Amendment protects the contents of communications transmitted and stored by an Internet Service Provider (ISP). In *United States v. Warshak*, the U.S. Court of Appeals for the Sixth Circuit, found that "in many contexts, the government infringes a reasonable expectation of privacy when it surreptitiously intercepts a telephone call through electronic means." 631 F.3d 266, 285 (6th Cir. 2010). The court reasoned that "[g]iven the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection." *Id.* at 285–86. (citation omitted). The court held that "a subscriber enjoys a reasonable expectation of privacy in the contents of emails 'that are stored with, or sent or received through, a commercial ISP.'" *Id.* at 288.

b) The Foreign Intelligence Surveillance Act of 1978 (FISA)[9]

21. The Foreign Intelligence Surveillance Act of 1978 (FISA) was enacted "to provide a statutory procedure for the authorization of applications for a court order approving the use of electronic surveillance to obtain foreign intelligence information" (*Foreign Intelligence Surveillance Act of 1978*, S. Rep. 95-604, pt. 1, at 3, *reprinted in* 1978 U.S.C.C.A.N. 3904, 3905 (1978)).

[9] FISA, in its totality, is in Tab 2 in the Booklet AB 1.

22. The FISA (in conjunction with the Electronic Communications Privacy Act (ECPA),[10] which consists of the Wiretap Act, the Stored Communications Act (SCA), and the Pen Register Act) was established as:

> *the exclusive means by which electronic surveillance and the interception of domestic wire, oral, or electronic communications may be conducted.*
>
> 50 U.S.C. § 1812.

23. The FISA's four basic surveillance provisions are: electronic surveillance (50 U.S.C. §§ 1801-1813), physical searches (50 U.S.C. §§ 1821-1829), pen/trap surveillance (50 U.S.C. §§ 1841-1846), and orders compelling production of tangible things including business records (50 U.S.C. §§ 1861-1864).

24. Electronic surveillance is defined in the FISA as:

> *(1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;*
>
> *(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of title 18;*
>
> *(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or*
>
> *(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.*
>
> 50 U.S.C. § 1801(f).

---

[10] ECPA is in Tab 3 in the Booklet AB 1.

25. The FISA traditionally limits and controls electronic surveillance and physical searches conducted **within the United States** for foreign intelligence purposes. The government, in general, has to apply for FISA Order from the Foreign Intelligence Surveillance Court (FISC) on the basis of 'probable cause' to believe that:

> ***(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power:*** *Provided, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and*
>
> ***(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;***
>
> 50 U.S.C. § 1805(a)(2) (emphasis added).

26. In 1998, and again in 2001, Congress added new provisions to FISA permitting electronic surveillance of both U.S. and non-U.S. persons, without a warrant, using "pen register" and "trap and trace" devices as well as business record requests. These provisions are known as Sections 405 and 215 of FISA, respectively (50 U.S.C. §§ 1845, 1861).

27. In 2008, Congress, however, added special new provisions authorizing access to international electronic communications to enable the targeting of non-U.S. persons located outside of the U.S. in Section 702 of the FISA Amendments Act (Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, §702, 122 Stat. 2436, 2438-2448 (2008) (codified at 50 U.S.C. § 1881a)). This section provides that

> *the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year . . . the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.*
>
> 50 U.S.C. § 1881a(a).

28. Under Section 702, the USIC is authorized to monitor **international communications**, even those involving U.S. persons, without a warrant, in order to "target" the communications of non-U.S. persons abroad and to acquire foreign intelligence information. Section 702 directives are not subject to any prior approval by the FISC. The Attorney General and the Director of National Intelligence must certify, among other things, that they have submitted to the FISC for approval 'targeting procedures' and 'minimization procedures' which indicate in general terms how communications will be targeted and dealt with once intercepted. 50 U.S.C. § 1881a(g)). Section 702 provides that the FISC "shall have jurisdiction to **review** a certification submitted" (50 U.S.C. § 1881a(i)(1)(A)). The 702 Order from the FISC does not involve the establishment of 'probable cause' or a review of whether any target is a foreign power or engaged in criminal activity, nor does the government have to identify the specific facilities or places at which electronic surveillance is directed.

29. Significantly, Section 702 also authorizes the USIC to access any of the international communications accessible to companies including electronic communications service providers in the U.S. without a warrant (see again 50 U.S.C. § 1881a). The government is authorized to

> *direct, in writing, an electronic communications service provider to—*
>
> *(A) immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition; and*
>
> *(B) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the acquisition or the aid furnished that such electronic communication service provider wishes to maintain.*
>
> 50 U.S.C. § 1881a(h)(1).

30. The FISA does not prohibit or control electronic surveillance that takes place outside of the U.S., except for certain data acquisitions that "intentionally target" a "United States person reasonably believed to be outside the United States" (under 50 U.S.C. § 1881c). Furthermore, many of the restrictions on access to, collection of, and dissemination of personal data in the FISA **only** apply to U.S. persons. The term "United States Persons" is defined as:

> *a citizen of the United States, an alien lawfully admitted for permanent residence..., an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power . . .*
>
> 50 U.S.C. § 1801(i).

It is my intention to discuss this issue in greater detail in submissions as Section 702 appears to be particularly germane to these proceedings.

31. Electronic communications service providers are compensated for carrying out these Section 702 directives under 50 U.S.C. § 1881a(h)(2) and are also released from liability "for providing any information, facilities, or assistance in accordance with a directive" under § 1881a(h)(3).

32. The only statutory limitations on surveillance under Section 702 are the acquisition limits, the targeting procedures, and the minimization procedures referred to above (50 U.S.C. §§ 1881a(b)–(e)).

33. Under Section 702, acquisition:

> *(1) may not intentionally target any person known at the time of acquisition to be located in the United States;*
>
> *(2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;*
>
> *(3) may not intentionally target a United States person reasonably believed to be located outside the United States;*
>
> *(4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and*
>
> *(5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.*
>
> 50 U.S.C. § 1881a(b).

34. The Attorney General, in consultation with the Director of National intelligence must adopt both targeting and minimization procedures (50 U.S.C. §§ 1881a(d)(1), (e)(1)). These procedures are subject to judicial review for their compliance with the statutory requirements (50 U.S.C. §§ 1881a(d)(2), (e)(2)). Targeting procedures must be

> *reasonably designed to-*
>
> *(A) ensure that any acquisition authorized . . . is limited to targeting persons reasonably believed to be located outside the United States; and*
>
> *(B) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.*
>
> 50 U.S.C. § 1881a(d)(1).

35. Minimization procedures must meet the requirements of § 1801(h) (50 U.S.C. § 1881a(e)(1)). Section 1801(h) defines minimization procedures as:

> *(1) specific procedures . . . that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of non-publicly available information concerning un-consenting United States persons consistent with the*

need of the United States to obtain, produce, and disseminate foreign intelligence information;

(2) procedures that require that non-publicly available information, which is not foreign intelligence information.... shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;

(3) notwithstanding [the above requirements] . . . procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and

(4) notwithstanding paragraphs [the above requirements] . . . with respect to any electronic surveillance approved . . . procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order . . . is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

50 U.S.C. §§ 1801(h)(1)–(4).

36. It is notable that neither the targeting nor the minimization procedures in Section 702 require protections for non-U.S. persons. Again, this is an issue which I intend to address in more detail in legal submissions. The Section 702 targeting procedures for the NSA were released in 2014 in a heavily redacted form.[11] A 2009 version has been made available.[12] A 2015 report by the Privacy and Civil Liberties Oversight Board (PCLOB) more recently elaborated on the procedures.[13] The Section 702 minimization procedures for the NSA from 2015 have

---

[11] PROCEDURES USED BY THE NATIONAL SECURITY AGENCY FOR TARGETING NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE OUTSIDE THE UNITED STATES TO ACQUIRE FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED (2014) is in Tab 4 in the AB 1 Booklet.

[12] PROCEDURES USED BY THE NATIONAL SECURITY AGENCY FOR TARGETING NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE OUTSIDE THE UNITED STATES TO ACQUIRE FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED (2009) is in Tab 5 in the AB 1 Booklet.

[13] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 41-66 (2014) is in Tab 6 in the AB 1 Booklet. The privacy and civil liberties oversight board (PCLOB) is an independent oversight agency within the U.S. executive branch. In the wake of the Snowden disclosures, PCLOB conducted a "comprehensive study" of the section 702 program at the request of the U.S. Congress and the President. The report described, analyzed, and recommended changes to the program.

been partially declassified.[14] Most relevantly, the procedures provide that acquisition of communications data will only be "effected in accordance" with an authorization of Attorney General and DNI and will "be conducted in a manner designed, to the greatest extent reasonably feasible, to minimize the acquisition of information not relevant to the authorized purpose of the acquisition."

37. Section 702 is the legal basis for the PRISM and Upstream surveillance programs referred to below. The FISA court has stated the "NSA acquires more than two hundred fifty million internet communications each year pursuant to Section 702." [*Redacted*], [docket no. redacted], slip op. at 9 (FISA Ct. Oct. 3, 2011).[15] Primarily through PRISM and Upstream programs. Both programs include the acquisition of communications content, but they have important distinguishing characteristics.

c) PRISM

38. The PRISM program involves directives to U.S. electronic communications service providers to grant the U.S. government access to internet communications. "The government sends a selector, such as an email address, to a United States-based electronic communications service provider" and that provider returns then the "communications sent to or from that selector to the government."[16] In 2011, "91 percent of the Internet communications that the NSA acquired each year" came from PRISM collection.[17] PRISM was a major part of the so-called Snowden revelations.

d) Upstream

39. There is another program operated under Section 702, called "Upstream", which is distinct from PRISM. The surveillance in the Upstream program is conducted "with the compelled assistance of providers that control the telecommunications 'backbone' over which telephone and Internet communications transit."[18] As a result, both telephone calls and Internet communications have been collected from backbone providers in vast quantities. A further distinguishing feature between PRISM and Upstream is that under Upstream "about" communications and multiple communications transactions (MCTs) are collected. As explained by PCLOB:

> *An 'about' communication is one in which the selector of a targeted person (such as that person's email address) is contained within the communication but the targeted person is not necessarily a participant in the communication . . . . An MCT is an Internet 'transaction' that contains more than one discrete communication within it. If one of the communications within an MCT is to, from,*

---

[14] MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED § 3(a) (2015) is in Tab 7 in the AB 1 booklet.

[15] [*Redacted*], [docket no. redacted], slip op. (FISA Ct, Oct. 3, 2011) is in Tab 8 in the AB 1 Booklet.

[16] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., *supra* note 13, at 7.

[17] *Id.* at 33-34.

[18] *Id.* at 7.

or 'about' a tasked selector, and if one end of the transaction is foreign, the NSA will acquire the entire MCT through upstream collection, including other discrete communications within the MCT that do not contain the selector.

40. The FISA Court has recognized that the U.S. government's collection of "about" communications is fundamentally different than other types of surveillance permitted under Section 702. In 2011, attorneys representing the USIC revealed to the FISA Court that:

> *acquisition of Internet communications through [the] upstream collection under Section 702 is accomplished by acquiring Internet 'transactions,' which may contain a single, discrete communication, or multiple discrete communications, including communications that are neither to, from, nor about targeted facilities.*
>
> [*Redacted*], [docket no. redacted], slip op. at 15 (FISA Ct. Oct. 3, 2011).

41. The FISA Court explained that "NSA's upstream Internet collection devices are generally incapable of distinguishing between transactions containing only a single discrete communication to, from, or about a tasked selector and transactions containing multiple discrete communications, not all of which may be to, from, or about a tasked selector." *Id.* at 31. The FISA Court emphasized that:

> *As a practical matter, this means that NSA's upstream collection devices acquire any Internet transaction transiting the device if the transaction contains a targeted selector anywhere within it.*
>
> *Id.*

42. The PCLOB report on Section 702 concluded that the surveillance technique used by the NSA to conduct "about" communication searches operates in such a way that every "person's communication will have been acquired because the government's collection devices examined the contents of the communication, without the government having held any prior suspicion regarding that communication."[19] In order to identify communications "about" a selector, the device must necessarily scan (and therefore acquire) all communications transmitted over that facility.

e) Article II of the U.S. Constitution

43. Electronic surveillance activities carried out by the NSA and other members of the USIC fall within the President's authority under Article II of the U.S. Constitution, which provides "[t]he executive power shall be vested in a President of the United States of America." U.S. CONST. ART II, § 1. The President exercises inherent powers as "commander in chief" and in the area of foreign affairs, and is charged to "take Care that the Laws be faithfully executed." U.S. CONST. ART II, §§ 2–3. The Constitution does not specifically detail the scope of the President's authority under this clause. Historically, Presidents have exercised power through

[19] *Id.* at 123.

executive orders and directives, such as the Presidential Policy Directive 28 and Executive Order 12333 described below. These orders, in conjunction with the legislative framework provided by statutes like FISA, establish rules for the USIC's activities. Covered entities must comply with both the statutes and executive orders where they both apply. Additionally, agencies such as the Department of Defense, of which the NSA is a component, fall within the executive branch and are subject to these rules. Agencies in turn develop internal policies and guidelines, also delineated below, which govern their activities.

f) Executive Order 12333[20]

44. Executive Order 12333 (EO 12333) sets out the President's rules and orders governing activities of the USIC. The Order outlines the roles of the different USIC departments and agencies (Part 1), regulates their conduct (Part 2), and outlines oversight, procedures, and definitions (Part 3) (Exec. Order No. 12,333: 40 Fed. Reg. 59,941 (Dec. 4, 1981), *reprinted as amended in* 73 Fed. Reg. 45,328 (2008) (July 30, 2008) [hereinafter EO 12333].) In general terms, the Order is the authority under which the National Security Agency (NSA) collects foreign intelligence. The Director of the National Security Agency is authorized under the Order to "collect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions" (EO 12333 § 1.7(c)(1)).

45. The Order also indicates that the Director of National Intelligence (DNI) serves "as the head of the Intelligence Community" and is charged with developing "guidelines for how information or intelligence is provided to or accessed by the Intelligence Community . . . and for how the information or intelligence may be used and shared by the Intelligence Community" (EO 12333 § 1.3). The Order, however, requires that the DNI carry out the responsibilities above "consistent with applicable law and with full consideration of **the rights of United States persons**, whether information is to be collected inside or outside the United States" (EO 12333 § 1.3(b)(19) (emphasis added)). Surveillance programs under the Order usually involve surveillance conducted **outside** the U.S. and do not have any judicial or FISA oversight.

46. The Director of the National Security Agency is authorized under the Order to "[c]ollect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions" (EO 12333 § 1.7(c)(1)).

47. The Order grants broad authority to USIC members to collect all forms of intelligence. The only collection limits imposed under the Order are outlined in Sections 2.3 and 2.4 (see below). Under the Order, "Intelligence includes foreign intelligence and counterintelligence" (EO 12333 § 3.5(f)). Foreign intelligence is defined broadly as "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign

[20] EO12333 is in Tab 9 in the AB 1 Booklet.

organizations, **foreign persons**, or international terrorists" (EO 12333 § 3.5(e) (emphasis added)).

48. Section 2.3 provides that USIC elements are authorized to:

> *collect, retain, or disseminate information concerning United States persons only in accordance with procedures established by the head of the Intelligence Community element concerned or by the head of a department containing such element and approved by the Attorney General.*
>
> EO 12333 § 2.3.

The Section provides that U.S. IC procedures "shall permit collection retention and dissemination" of ten types of information (EO12333 §§ 2.3(a)-(j)). The Section also authorizes USIC elements to:

> *disseminate information to each appropriate element within the Intelligence Community for purposes of allowing the recipient element to determine whether the information is relevant to its responsibilities and can be retained by it, except that information derived from signals intelligence may only be disseminated or made available to Intelligence Community elements in accordance with procedures established by the Director in coordination with the Secretary of Defense and approved by the Attorney General.*
>
> EO 12333 § 2.3.

49. Section 2.4 requires that U.S. IC elements:

> ***Shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad**. Elements of the Intelligence Community are not authorized to use such techniques as electronic surveillance, unconsented physical searches, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the Intelligence Community element concerned or the head of a department containing such element and approved by the Attorney General, after consultation with the Director. Such procedures shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes.*
>
> EO 12333 § 2.4 (emphasis added).

g) PPD-28[21]

50. Presidential Policy Directive 28 (PPD-28) is a presidential order, adopted after the Snowden revelations, that imposes certain restrictions on U.S. signals intelligence activities implicating personal information **regardless of the person's nationality or location** (THE WHITE HOUSE, PRESIDENTIAL POLICY DIRECTIVE 28: SIGNALS INTELLIGENCE ACTIVITIES (2014) [hereinafter PPD-28]).

51. Section 1 of PPD-28 states four "principles" governing collection via signals intelligence:

> *(a) The collection of signals intelligence shall be authorized by statute or Executive Order, proclamation, or other Presidential directive, and undertaken in accordance with the Constitution and applicable statutes, Executive Orders, proclamations, and Presidential directives.*
>
> *(b) Privacy and civil liberties shall be integral considerations in the planning of U.S. signals intelligence activities. The United States shall not collect signals intelligence for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion. Signals intelligence shall be collected exclusively where there is a foreign intelligence or counterintelligence purpose to support national and departmental missions and not for any other purposes.*
>
> *(c) The collection of foreign private commercial information or trade secrets is authorized only to protect the national security of the United States or its partners and allies. It is not an authorized foreign intelligence or counterintelligence purpose to collect such information to afford a competitive advantage to U.S. companies and U.S. business sectors commercially.*
>
> *(d) Signals intelligence activities shall be as tailored as feasible. In determining whether to collect signals intelligence, the United States shall consider the availability of other information, including from diplomatic and public sources. Such appropriate and feasible alternatives to signals intelligence should be prioritized.*
>
> PPD-28 §§ 1(a)–(c).

52. The Office of the Director of National Intelligence ("ODNI") has explained that pursuant to the fourth principle, "the Intelligence Community takes steps to ensure that even when we cannot use specific identifiers to target collection, the data to be collected is likely to contain foreign intelligence that will be responsive to requirements articulated by U.S. policy-makers pursuant to the process explained in my earlier letter, and minimizes the amount of non-

[21] PPD-28 is in Tab 10 in the AB 1 Booklet.

pertinent information that is collected."[22] As an example, where specific selectors are not available but a group is being targeting, the U.S. "might choose to target that group by collecting communications to and from that region for further review and analysis to identify those communications that relate to the group."

53. Section 2 governs signals intelligence collected in "bulk." PPD-28 defines "bulk" collection as "the authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.)" (PPD-28 § 2 n.5). Section 2 allows for the collection of "signals intelligence in bulk in certain circumstances" which "may . . . result in the collection of information about persons whose activities are not of foreign intelligence or counterintelligence value" (PPD-28 § 2).

54. Section 2 does not impose any limits on access to or acquisition of communications, only limits on the *use* of acquired communications. Section 2 requires that that the U.S. "shall use" "non-publicly available signals intelligence" collected in "bulk" for only six purposes:

> *(1) espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests;*
>
> *(2) threats to the United States and its interests from terrorism;*
>
> *(3) threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction;*
>
> *(4) cybersecurity threats;*
>
> *(5) threats to U.S. or allied Armed Forces or other U.S or allied personnel; and*
>
> *(6) transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes named in this section.*
>
> PPD-28 § 2.

55. These limitations for bulk collection are also themselves subject to an exception; they "do not apply to signals intelligence data that is temporarily acquired to facilitate targeted collection" (PPD-28 § 2 n.5).

56. PPD-28 extended EO 12333's limits on dissemination and retention of personal information, but did not extend the collection limits. Specifically, in reference to EO 12333, PPD-28 mandates that for all individuals:

---

[22] Annexes to the Commission Implementing Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield at 95 (Dec. 7, 2016) [hereinafter Annexes] is in Tab 11 in the AB 1 Booklet.

Dissemination: Personal information shall be disseminated only if the dissemination of comparable information concerning U.S. persons would be permitted under section 2.3 of Executive Order 12333.

Retention: Personal information shall be retained only if the retention of comparable information concerning U.S. persons would be permitted under section 2.3 of Executive Order 12333 and shall be subject to the same retention periods as applied to comparable information concerning U.S. persons. Information for which no such determination has been made ***shall not be retained for more than 5 years, unless the DNI expressly determines that continued retention is in the national security interests of the United States.***

PPD-28 § 4(a)(i) (emphasis added).

h) USSID 18[23]

57. The NSA has adopted a set of procedures, United States Signals Intelligence Directive SP0018, pursuant to EO12333 that govern signals intelligence activities (NAT'L SEC. AGENCY, USSID SP0018: LEGAL COMPLIANCE AND U.S. PERSONS MINIMIZATION PROCEDURES (2011) [hereinafter USSID 18]). The purpose of USSID 18 is to establish rules such that "signals intelligence (SIGINT) operations are conducted pursuant to procedures which meet the reasonableness requirements of the Fourth Amendment" (USSID 18 § 1.1.) The rules in USSID 18 are based on the premise that "The Fourth Amendment to the United States Constitution protects all **U.S. persons** anywhere in the world and all persons **within the United States** from unreasonable searches and seizures by any person or agency acting on behalf of the U.S. Government" (USSID 18 § 1.1) (emphasis added).

58. The USSID 18 rules limit the collection of "communications to, from or about U.S. PERSONS or persons or entities in the U.S." (USSID 18 § 3.1).

59. The NSA updated USSID 18 in 2015 in accordance with PPD-28 by issuing supplemental procedures focused on signal intelligence activities directed at **non-US persons**[24] (NAT'L SEC. AGENCY, USSID SP0018: SUPPLEMENTAL PROCEDURES FOR THE COLLECTION, PROCESSING, RETENTION, AND DISSEMINATION OF SIGNALS INTELLIGENCE INFORMATION AND DATA CONTAINING PERSONAL INFORMATION OF UNITED STATES PERSONS (2015) [hereinafter USSID 18 Supplemental Procedures]).

60. The supplemental procedures are focused primarily on the use of "personal information" of non-U.S. persons that has already been collected. The rules state that "[i]f the USSS COLLECTS personal information of non-U.S. persons, it will process, analyze, disseminate, and retain such personal information only in accordance with these Supplemental Procedures" (USSID 18 Supplemental Procedures § 3.3). The term "personal information" includes "the same types of information covered by 'information concerning U.S. persons'

[23] USSID 18 is in Tab 12 of the AB 1 Booklet.
[24] USSID 18 Supplemental Procedures are in Tab 13 of the AB 1 Booklet.

under Section 2.3 of Executive Order 12333" (USSID 18 Supplemental Procedures § 3.3). Information concerning U.S. persons is not defined in EO 12333, but is defined in the Department of Defense manual (that governs NSA and other Department of Defense intelligence activities) as:

> *Information that is reasonably likely to identify one or more specific U.S. persons. USPI may be either a single item of information or information that, when combined with other information, is reasonably likely to identify one or more specific U.S. persons . . .*
>
> DODM § G.2.

III REMEDIES AND EU CITIZENS' SURVEILLANCE CLAIMS

61. EU citizens whose personal data has been transferred to the U.S. have limited remedies available where their claims arise from access to, use of, or dissemination of their private communications or other personal data. Statutory remedies include the Judicial Redress Act, FISA § 1810, the Stored Communications Act § 2712, FISA §§ 1806 and 1809, the Fourth Amendment, among few other statutory provisions. None of these statutory remedies provide a means of redress for bulk surveillance conducted under Section 702 or EO 12333.

a) Judicial Redress Act[25]

62. The Judicial Redress Act, passed in 2015, extends to a limited group of non-US persons, certain remedies under the Privacy Act of 1974 relating to personal information held by federal agencies.

63. The Privacy Act of 1974[26] protects personal information of an "individual," defined as "a citizen of the United States or an alien lawfully admitted for permanent residence" maintained by U.S. federal agencies (5 U.S.C. § 552a(2)). The statute provides that such an individual may bring a civil action against an agency where the agency:

> *(A) makes a determination . . . not to amend an individual's record in accordance with his request, or fails to make such review in conformity with that subsection;*
>
> *(B) refuses to comply with an individual request [for access to her record or information pertaining to her] . . .*
>
> *(C) fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of*

[25] Judicial Redress Act is in Tab 14 of the AB 1 booklet.
[26] Privacy Act of 1974 is in Tab 15 of the AB 1 booklet.

such record, and consequently a determination is made which is adverse to the individual; or

(D) fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual . . .

5 U.S.C. § 552a(g)(1)(A)–(D).

64. The Judicial Redress Act provides a cause of action to "covered persons" for Privacy Act violations of:

(1) section 552a(g)(1)(D) of title 5, United States Code, but only with respect to disclosures intentionally or willfully made in violation of section 552a(b) of such title; and

(2) subparagraphs (A) and (B) of section 552a(g)(1) of title 5, United States Code, but such an action may only be brought against a designated Federal agency or component.

Judicial Redress Act, Pub. L. 114-126, § 2(a), 130 Stat. 282 (2016).

65. The Judicial Redress Act establishes that, for those specific causes of action, "**a covered person** shall have the same rights, and be subject to the same limitations, including exemptions and exceptions, as an individual has and is subject to under" the Privacy Act (Judicial Redress Act § 2(c) (emphasis added)).

66. The Judicial Redress Act defines a "covered person" as "a natural person . . . who is a citizen of a 'covered country'" (Judicial Redress Act § 2(h)(3)). A "covered country" is defined as a country "or regional economic integration organization, or member country of such organization" designated by the Attorney General under the rules outlined in the Act. (Judicial Redress Act § 2(h)(2)). The Act provides that the Attorney General may:

with the concurrence of the Secretary of State, the Secretary of the Treasury, and the Secretary of Homeland Security, designate a foreign country or regional economic integration organization, or member country of such organization, as a 'covered country' for purposes of this section if—

(A)

(i) the country or regional economic integration organization, or member country of such organization, has entered into an agreement with the United States that provides for appropriate privacy protections for information shared for the purpose of preventing, investigating, detecting, or prosecuting criminal offenses; or

(ii) the Attorney General has determined that the country or regional economic integration organization, or member country of such organization, has effectively shared information with the United States for the purpose of preventing, investigating, detecting, or prosecuting criminal offenses and has appropriate privacy protections for such shared information;

(B) the country or regional economic integration organization, or member country of such organization, permits the transfer of personal data for commercial purposes between the territory of that country or regional economic organization and the territory of the United States, through an agreement with the United States or otherwise; and

(C) the Attorney General has certified that the policies regarding the transfer of personal data for commercial purposes and related actions of the country or regional economic integration organization, or member country of such organization, do not materially impede the national security interests of the United States.

Judicial Redress Act § 2(d)(1).

67. The Act also authorizes the Attorney General to "revoke the designation" if he or she finds the requirements for designation falter in the future or if the entity "impedes the transfer of information (for purposes of reporting or preventing unlawful activity) to the United States by a private entity or person" (Judicial Redress Act § 2(d)(2)). The designation and removal determinations "shall not be subject to judicial or administrative review" (Judicial Redress Act § 2(f)).

68. The specific causes of action in the Privacy Act are also reduced in the Judicial Redress Act.

69. As to the Privacy Act's causes of action in §§ 55a2(g)(1)(A)–(B), the Judicial Redress Act only allows comparable suits against "designated agencies" (Judicial Redress Act § 2(a)(2). The Attorney General shall "determine whether an agency or component thereof is a 'designated Federal agency or component' for purposes of this section." (Judicial Redress Act § 2(e)). The designation of a federal agency or component "shall not be subject to judicial or administrative review (Judicial Redress Act § 2(f)).

70. The Judicial Redress Act does <u>not</u> provide for the possibility of a civil action with respect to Privacy Act section 552a(g)(1)(C) (set out above).

71. With respect to the Privacy Act cause of action § 552a(g)(1)(D), the Judicial Redress Act only provides an analogous right with respect to disclosures <u>intentionally or willfully</u> made in violation of § 552a(b) (Judicial Redress Act § 2(a)(1)). The Privacy Act section 552a(b) requires that "[n]o agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a

written request by, or with the prior written consent of, the individual to whom the record pertains" unless one of twelve enumerated exceptions apply" (5 U.S.C. § 552a(b)).

b) FISA Sections 1810 and 1809

72. Section 1810 of FISA provides a civil cause of action for damages to certain persons subjected to a misuse of electronic surveillance.

73. FISA § 1810 provides that:

> *an aggrieved person, other than a foreign power or an agent of a foreign power . . . who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of section 1809 . . . shall have a cause of action against any person who committed such violation . . . .*
>
> 50 U.S.C. § 1810.

74. Accordingly, an individual can only bring a claim under FISA § 1810 in circumstances where they can establish a "violation of section 1809" (50 U.S.C. § 1810). Section 1809 makes an individual guilty of a criminal offense if he or she intentionally:

> *(1) engages in electronic surveillance under color of law except as authorized by this chapter, chapter 119, 121, or 206 of title 18, or any express statutory authorization that is an additional exclusive means for conducting electronic surveillance under section 1812 of this title;*
>
> *(2) discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by this chapter, chapter 119, 121, or 206 of title 18, or any express statutory authorization that is an additional exclusive means for conducting electronic surveillance under section 1812 of this title.*
>
> 50 U.S.C. § 1809(a).

75. The definition of "electronic surveillance" is strictly limited under FISA. Section 702 also provides an "express statutory authorization" for electronic surveillance under FISA § 1809. Therefore any surveillance that (1) takes place outside the United States (or otherwise not within FISA's "electronic surveillance" definition) or (2) is conducted pursuant to directives issued under Section 702 would not be actionable under FISA § 1810. It is not clear that violations of the targeting or minimization procedures adopted under a Section 702 authorization order would be redressable under FISA § 1810.

76. There have not been many cases brought under FISA § 1810. However, one U.S. Court of Appeals has found that U.S. government agencies, and government employees acting in their

official capacity, are immune from liability under the provision. In *Al-Haramain Islamic Found., Inc. v. Obama*, U.S. Court of Appeals for the Ninth Circuit held that "we do not interpret the reference to 'person' in § 1810 to mean that a government employee is liable in his official capacity." *Al-Haramain Islamic Found., Inc. v. Obama*, 705 F.3d 845, 854–55 (9th Cir. 2012).

c) The Stored Communications Act, Section 2712[27]

77. Section 2712, of the Stored Communications Act, provides:

> *Any person who is aggrieved by any willful violation of this chapter or of chapter 119 of this title or of sections 106(a), 305(a), or 405(a) of the Foreign Intelligence Surveillance Act . . . may commence an action in United States District Court against the United States to recover money damages. In any such action, if a person who is aggrieved successfully establishes such a violation . . . the Court may assess as damages.*
>
> 18 U.S.C. § 2712.

78. In order to bring an action against the United States under the Stored Communications Act, an individual must establish a "willful violation" of either (1) the Stored Communications Act,[28] (2) the Wiretap Act,[29] (3) the traditional FISA minimization procedures,[30] (4) the FISA physical search minimization procedures,[31] or (5) the FISA pen register and trap and trace minimization procedures.[32]

79. The Stored Communications Act prohibits "electronic communications service" and "remote computing service" providers from divulging "the contents of a communication" to "any person" or to divulge "a record or other information pertaining to a subscriber to or customer of such service" to "any government entity" except in certain circumstances (18 U.S.C. § 2702). Courts have held that the protections granted under this section are limited by numerous definitions and exceptions. By definition, the United States could not be charged with a "willful violation" of § 2702 because the section only prohibits actions of *service providers*.

80. The Stored Communications Act includes a broader prohibition on "[u]nlawful access to stored communications" (18 U.S.C. § 2701). The section prescribes punishments for:

---

[27] The Stored Communications Act is in Tab 3 of the AB1 Booklet (within ECPA).
[28] 18 U.S.C. §§ 2701 et seq.
[29] 18 U.S.C. §§ 2511 et seq.
[30] 50 U.S.C. § 1806(a). The traditional FISA minimization procedures are focused on limiting the use of information "concerning any United States person." *Id.*
[31] 50 U.S.C. § 1825(a).
[32] 50 U.S.C. § 1845(a). In the context of pen trap/trace surveillance, a 2712 cause of action would arise from use or disclosure of information acquired concerning a U.S. person without that persons consent in violation of the provisions for use and disclosure of § 1845 (allowing disclosure for certain law enforcement purposes, in certain government proceedings, and related purposes) or for unlawful purposes. *Id.*

whoever—

> *(1) Intentionally accesses without authorization a facility through which an electronic communication service is provided; or*
>
> *(2) intentionally exceeds an authorization to access that facility;*
>
> *and thereby obtains, alters or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system . . .*
>
> 18 U.S.C. § 2701(a).

81. There are limitations on the Stored Communications Act "unauthorized access" prohibition. The prohibition does not, for instance, apply "to conduct authorized . . . (1) by the person or entity providing a wire or electronic communications service . . . or (3) in section 2703, 2704 or 2518 of [18 U.S.C.]" (18 U.S.C. § 2701). Electronic communications service providers are required to "immediately provide the Government with all . . . assistance necessary to accomplish the acquisition" in response to a directive issued under Section 702 of the FISA, and are released from all liability for doing so (50 U.S.C. § 1881a(h)). Providers and "their officers, employees, and agents, landlords, custodians, or other persons" are also authorized to provide assistance pursuant to FISA Court orders or certifications from the Attorney General under 18 U.S.C. § 2511(2)(a).

82. In addition, the unauthorized access provision does not prohibit a service provider from divulging communications that are not held "in electronic storage by that service" provider (18 U.S.C. § 2701(a)(1)). Electronic storage is defined as:

> *(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and*
>
> *(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication;*
>
> 18 U.S.C. § 2510(17).

83. Even where communications are held by a service provider in electronic storage, a United States government entity may "require a provider" to "disclose the contents of a wire or electronic communication" using "an administrative subpoena" if the communications have "been in electronic storage in an electronic communications system for more than one hundred and eighty days" (18 U.S.C. §§ 2703(a)–(b)).

84. Section 2712 does not provide a remedy applicable to a violation of the provisions for the compelled production of tangible things under FISA or for Section 702 FISA surveillance.

85. In order to seek remedies against the United States under § 2712, an individual must first present the claim "to the appropriate department or agency under the procedures of the Federal Tort Claims Act" (18 U.S.C. § 2712(b)(1)).

d) The Privacy Shield Ombudsperson

86. The Privacy Shield also includes remedies provisions that provide for an ombudsman mechanism available to EU citizens subject to trans-border data flows. The mechanism will "facilitate the processing of requests relating to national security access to data transmitted from the EU to the United States," including through standard contractual clauses.[33] The Ombudsperson reports directly to the Secretary of State.[34]

87. Through this mechanism, individual EU citizen requests go through authorities in EU states, to an EU centralized complaint body, and then to the Ombudsperson. In the case of requests related to surveillance, "the Privacy Shield Ombudsperson will be able to cooperate with one of the independent oversight bodies with investigatory powers" and the "request need not demonstrate the requester's data has in fact been accessed by the United States Government through signal intelligence activities."[35] Additionally, a request that alleges a "violation of law or other misconduct will be referred to the appropriate United States Government body, including independent oversight bodies, with the power to investigate the respective request and address non- compliance."[36]

88. Once an individual has filed a complaint, the Ombudsperson "will provide a response to the submitting EU individual complaint handling body confirming (i) that the complaint has been properly investigated, and (ii) that the U.S. law, statutes, executives orders, presidential directives, and agency policies, providing the limitations and safeguards described in the ODNI letter, have been complied with, or, in the event of non-compliance, such non-compliance has been remedied."[37] However, the Ombudsperson will "neither confirm nor deny whether the individual has been the target of surveillance nor will the Privacy Shield Ombudsperson confirm the specific remedy that was applied."[38]

e) The Fourth Amendment

89. The Fourth Amendment (set out above) provides protection from unreasonable searches and seizures to individuals in the United States. Fourth Amendment violations can be redressed through the suppression of evidence via the "exclusionary rule." In both state and federal courts "the Fourth Amendment bar[s] the use of evidence secured through an illegal search and seizure if evidence is obtained in violation of the Fourth Amendment." *Mapp v. Ohio*, 367 U.S. 643, 648 (1961) (citation omitted). Additionally, a "*Bivens*" action can be brought

---

[33] Annexes, *supra* note 23, at 52.
[34] *Id.* at 53.
[35] *Id.* at 53-54.
[36] *Id.* at 56.
[37] *Id.* at 55.
[38] *Id.*

against an individual "federal agent acting under color of his authority gives rise to a cause of action for damages consequent upon" his conduct violating the Fourth Amendment. *Bivens v. Six Unknown Named Agents*, 403 U.S. 388, 389 (1971).

90. However, in general, foreigners located abroad are not protected by the Fourth Amendment.[39] In order to assert Fourth Amendment rights, an individual must have a "significant voluntary connection with the United States." *United States v. Verdugo-Urquidez*, 494 U.S. 259, 271 (1990).

f) Other statutory remedies

91. Other possible statutory remedies arise under the Computer Fraud and Abuse Act (CFAA), the Right to Financial Privacy Act (RFPA), and the Freedom of Information Act (FOIA).

92. The CFAA provides a civil action to any person who "suffers damage or loss" because of a violation of the statute where the conduct involves one of five factors listed in sections 1030(c)(4)(A)(i)(I)–(V), and the claim is brought within two years of "the act complained of or the date of the discovery of the damage" (18 U.S.C. § 1030(g)). Damages for a violation involving only the first factor are limited to economic damages (18 U.S.C. § 1030(g)). The said five factors are:

> *(I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;*
>
> *(II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;*
>
> *(III) physical injury to any person;*
>
> *(IV) a threat to public health or safety;*
>
> *(V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security;*
>
> 18 U.S.C. § 1030 (c)(4)(A)(i)(I)(I)–(V).

93. The RFPA limits disclosures of private financial records held by certain financial institutions to government authorities. It provides:

---

[39] The extraterritorial application of the Fourth Amendment may be in flux. *Hernandez v. United States*, 785 F.3d 117 (5th Cir. 2015), *cert. granted sub nom. Hernandez v. Mesa*, 84 U.S.L.W. 3060 (U.S. Oct. 11, 2016) (No. 15–118).

> *Except as provided by [RFPA] . . . no Government authority may have access to or obtain copies of, or the information contained in the financial records of any customer from a financial institution unless the financial records are reasonably described and – such customer has authorized such disclosure . . . such financial records are disclosed in response to an administrative subpoena or summons . . . search warrant . . . judicial subpoena . . . or . . . a formal written request.*
>
> 12 U.S.C. § 3402.

94. The Freedom of Information Act (FOIA) requires that "each agency, upon any request for records which (i) reasonably describes such records and (ii) is made in accordance with published rules stating the time, place, fees (if any), and procedures to be followed, shall make the records promptly available to any person" (5 U.S.C. § 552(a)(3)). This requirement is subject to nine exemptions. Of particular relevance, these exemptions cover certain "records or information compiled for law enforcement purposes" (5 U.S.C. § 552(b)(7)) and matters which are "(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order" (5 U.S.C. § 552(b)(1)).

IV Obstacles to Redress

95. Two significant hurdles to redress in privacy and surveillance cases are the "standing" doctrine and the "state secrets" privilege.

a) Standing

96. Article III of the U.S. Constitution provides that the power of federal courts extends only to "cases" or "controversies." U.S. CONST. art. III, § 2. The U.S. Supreme Court has interpreted this case and controversy requirement such that a plaintiff must establish an "irreducible constitutional minimum of standing" in order to be permitted to bring an action in federal court. The standing requirement has three elements:

> *First, the plaintiff must have suffered an "injury in fact"—an invasion of a legally protected interest which is (a) concrete and particularized . . . and (b) "actual or imminent, not 'conjectural' or 'hypothetical,'" . . . . Second, there must be a causal connection between the injury and the conduct complained of—the injury has to be "fairly . . . trace[able] to the challenged action of the defendant, and not . . . th[e] result [of] the independent action of some third party not before the court." . . . Third, it must be "likely," as opposed to merely "speculative," that the injury will be "redressed by a favorable decision.*
>
> *Lujan* v. *Defenders of Wildlife*, 504 U. S. 555, 560–61 (1992) (citations omitted).

97. The U.S. Supreme Court has recently found that the standing doctrine limits the availability of judicial redress in privacy and surveillance cases. In *Clapper v. Amnesty Int'l USA*, a case

in which EPIC served as *amicus curiae*, the U.S. Supreme Court held that a group of attorneys, advocates, and others who routinely communicated with foreigners abroad could not bring a challenge to the U.S. government's Section 702 surveillance program. 133 S. Ct. 1138 (2013). The Court found that the plaintiffs' claim that their foreign communications were being collected under the Section 702 program was "too speculative to satisfy the well-established requirement that threatened injury must be 'certainly impending.'" *Id.* at 1143. The Court went on to hold that even if the plaintiffs could show that the interception of their communications was "certainly impending, they would still not be able to establish that this injury is fairly traceable to [Section 702]."

98. As apparent from the recent U.S. Supreme Court judgment *Spokeo v. Robins*, there are further limitations to the ability of individuals to seek redress of data privacy claims in federal court. 136 S. Ct. 1540 (2016).

b) State Secrets Privilege

99. The U.S. Supreme Court has held that when there is a "reasonable danger that compulsion of the evidence will expose military matters which, in the interest of national security, should not be divulged," that evidence is privileged. *United States v. Reynolds*, 345 U.S. 1, 10 (1953). This evidentiary privilege must be asserted in a case by the "head of the department which has control over the matter, after actual personal consideration by that officer," and the court then evaluates whether "circumstances are appropriate for the claim of privilege... without forcing a disclosure" of the material. *Id.* at 8.

100. In 2009, the Department of Justice issued a policy limiting government invocation of the state secrets privilege "to the extent necessary to protect against the risk of significant harm to national security."[40] While this is an evidentiary privilege, if state secrets are integral to the case—for example, where they would be necessary to establish standing, or where the very subject matter of the suit is privileged—a court will simply refuse to hear the case.

101. The state secrets privilege is implicated in most surveillance and national security cases.[41] For instance, in *Jewel v. NSA*, plaintiffs challenged the Section 702 "upstream" surveillance program on Fourth Amendment grounds. *Jewel v. Nat'l Sec. Agency*, No. C 08-04373 JSW, WL 5452925 (N.D. Cal. Feb 10, 2015). The case was dismissed where the court found insufficient evidence to support standing based on the public details of the program, and where litigating the standing issue and the Government's substantive defenses would require revealing details of the Upstream program subject to the state secrets privileged. *Id.* at *3-5.

---

[40] MEMORANDUM FROM ERIC HOLDER, DEPARTMENT OF JUSTICE, POLICIES AND PROCEDURES GOVERNING INVOCATION OF THE STATE SECRETS PRIVILEGE (2009).

[41] *See Mohamed v. Jeppesen DataPlan, Inc.*, 614 F.3d 1070 (9th Cir. 2010) (dismissal of challenge to extraordinary rendition program under the state secrets privilege); *Fazaga v. Fed. Bureau of Investigation*, 884 F.Supp.2d 1022 (C.D. Cal. 2012) (dismissal under the state secrets privilege); *Terkel v. AT&T Corp.*, 441 F.Supp.2d 899 (N.D. Ill. 2006) (dismissal of challenge to company participation in NSA surveillance for lack of standing after applying the state secrets privilege); *Al-Haramain Islamic Found. Inc. v. Bush,* 507 F.3d 1190 (9th Cir. 2007) (remanding on other grounds, but finding that the challenge to NSA surveillance could have been dismissed because without the privileged material the plaintiff could not establish standing).