ENCRYPTED MESSAGING APPS IN THE AGE OF TERRORISM AND SNOWDEN: SAVIOR OR SAFE HAVEN?

A Thesis
submitted to the Faculty of
The School of Continuing Studies
and of
The Graduate School of Arts and Sciences
in partial fulfillment of the requirements for the
degree of
Master of Arts in Liberal Studies

By

James Colraine, B.S.

Georgetown University
Washington, D.C.
April 1, 2016

ENCRYPTED MESSAGING APPS IN THE AGE OF TERRORISM AND SNOWDEN: SAVIOR OR SAFE HAVEN?

James Colraine, B.S.

Mentor: Estelle Hofschneider, J.D.

ABSTRACT

Communications technology is fundamentally changing the way people live their lives. Smartphones have become mobile computers. Vast amounts of personal information are stored and collected on the mobile devices that we carry. A major debate is now taking place within the United States on the balance between privacy and security—a debate that was galvanized in 2013 after Edward Snowden's revelations of massive US government surveillance against technology used by many people not just in the United States, but worldwide. Lately, the debate has centered on the US government's claim, articulated by FBI Director James Comey, that law enforcement agencies are now "going dark" on potential evidence of serious crimes, including terrorism. The government argues it is unable to access some digital information, even with a valid legal warrant, due to the recent implementation of encryption across many mobile communications platforms. Because the communications are encrypted, technology companies served with a warrant simply respond that even they themselves cannot access the data. The move towards encryption for some companies was motivated, at least in part, by business reasons, as well as privacy rights concerns. After the 2013 revelations, many companies sought to distance themselves from the US government as internationally, technology companies were being painted with a broad brush that they

assisted the government in carrying out the mass surveillance. Recently, secure communication applications such as SnapChat, Wickr and Telegram have increased in popularity due to their ability to provide instantaneous encrypted communications and the ability to auto delete data.[1]

In 2015 and 2016, adherents of the Islamic State of Iraq and the Levant (ISIL) executed major terrorist attacks in the cities of Paris, Brussels, and San Bernadino. In several of these attacks, the perpetrators utilized secure communication applications to plan and coordinate the killing of innocent people.[2] In a 2015 attack carried out in Garland, Texas, the perpetrator had communicated with an ISIL attack plotter overseas. The government was never able to decrypt their secure communications, thus losing valuable intelligence on how individuals in the United States may be contacted, recruited and possibly trained to conduct attacks from ISIL overseas. Despite the government's concerns, many technology companies maintain that privacy rights and the benefits of secure communications to a free society trump the benefits provided by potential governmental access to all communications.

This paper will explore both sides of the debate with regard to the use of secure communications applications and potential solutions that may allow the government to get the information they need while preserving the privacy needs of the individual and the

[1] Hilton Collins, "3 Technologies Claiming to Secure Messages in the Post-Snowden Era," *Government Technology*, July 10, 2014, accessed March 5, 2016, http://www.govtech.com/videos/3-Techs-Claim-to-Secure-Messages-in-the-Post-Snowden-Era.html.

[2] Rebecca Kaplan, "Encrypted Messages: Does the Government Need a Way In?," *CBS News*, November 16, 2015, accessed March 12, 2016, http://www.cbsnews.com/news/paris-attacks-encrypted-messages-does-the-government-need-a-way-in/.

economic competitiveness of technology companies at home and abroad. However, as technology continues to evolve, the debate will likely continue to shift as each side tries to figure out the right balance for their needs.

ACKNOWLEDGMENTS

I would like to thank my mentor, Estelle Hofschneider, who generously provided her time, expertise and sage guidance on this paper. I can't begin to tell you how much your help has meant. I would also like to thanks Dr. Anne Ridder, who has been with me every step of the way on this process and has gone above and beyond in helping me complete my requirements while I was relocated 3,000 miles away from campus. I'm truly indebted to her.

TABLE OF CONTENTS

ILLUSTRATIONS

Figures

Tables

CHAPTER 1

INTRODUCTION

Since the revelation of massive government bulk data surveillance on Americans and foreign targets in 2013, a shift has occurred within the technology community and the privacy activist community to address what they view as an assault on personal liberties. In an article from *The Nation* entitled, "Can Encryption Save Us?", author Eleanor Saitta notes that in the aftermath of the Edward Snowden leaks, privacy advocates and engineers in the technology community "told the public to trust math—encryption—not politics or law to protect their privacy."[1] According to Saitta, the track record of reining in US surveillance through the law was "abysmal," with "no proven instances of a law permanently removing an operational, cost effective, productive foreign-surveillance capability on human rights or constitutional grounds."[2] On the other end of the spectrum, Former NSA Director General Michael Hayden believes that the NSA and by extension, the US Government have been wrongfully accused. In an interview with the *Financial Review*, General Hayden stated the "NSA has been fulfilling its responsibilities to the nation and yet it is being constantly vilified and misrepresented in the press. The media have presented the unauthorized leaks of stolen US intelligence—most of which has nothing to do with American citizens and privacy but instead

[1] Eleanor Saitta "Can Encryption Save Us?" *Nation* 300, no. 24 (June 15, 2015): 16-18. *Academic Search Premier*, EBSCO*host*, accessed February 29, 2016.

[2] Ibid.

represents legitimate foreign intelligence gathering—in such a way that the public is incorrectly led to believe that NSA, and its people, are doing something illegal or improper."[3]

Yet, trusting in math instead of the Government, companies such as Microsoft, Apple, Google and Yahoo have incorporated enhanced encryption services on their platforms.[4] Even going as far as implementing full end-to-end encryption, where even if served a valid court order or warrant from a magistrate judge to turn over information, the companies would be unable to comply as they do not possess the encryption keys to unlock the data.[5] In other words, law enforcement agencies would be given the data, but it would be completely indecipherable.[6]

The inability to meaningfully serve legal process on encrypted communications services has the law enforcement and intelligence communities concerned with the possibility of being blind to threats posed by terrorists, spies, pedophiles, and criminal

[3] Christopher Joye, "Interview Transcript: Former Head of the NSA and Command of the US Cyber Command, General Keith Alexander," *Financial Review*, May 8, 2014, accessed March 7, 2016, http://www.afr.com/technology/web/security/interview-transcriptformer-head-of-the-nsa-and-commander-of-the-us-cyber-command-general-keith-alexander-20140507-itzhw.

[4] Cammy Harbison, "Microsoft Adds Enhanced Encryption To Outlook Email And Other Cloud Services, Increasing Privacy And Security," *iDigital Times*, July 2, 2014, accessed March 7, 2016, http://www.idigitaltimes.com/microsoft-adds-enhanced-encryption-outlook-email-and-other-cloud-services-increasing-privacy-and.

[5] Matthew Green, "Here Come the Encryption Apps!," *A Few Thoughts on Cryptographic Engineering Blog*, March 9, 2013, accessed February 29, 2016, http://blog.cryptographyengineering.com/2013/03/here-come-encryption-apps.html.

[6] Benjamin Wittes, "Jim Comey, ISIS, and "Going Dark"," *Lawfare Blog*, July 1, 2015, accessed March 9, 2016, https://www.lawfareblog.com/jim-comey-isis-and-going-dark.

cyber actors, among others.[7] If encrypted communication platforms become "virtual safe havens," government authorities fear—and rightly so— bad actors will rush to adopt those communication channels in order to evade law enforcement detection and plan their activities without fear of discovery.[8] To those charged with protecting the nation from terrorist attacks, this freedom to plot would not only facilitate, but could also arguably encourage, future attacks. The terrorist attacks in Paris in November 2015 are thought to have been planned using encrypted communications.[9] These attacks underscore the government's position that bad actors will flock to these platforms for their operational activities and that law enforcement visibility on these communications is not only necessary to apprehend all those responsible, but is also crucial to prevent future attacks.

In testimony before the Homeland Security Committee of the US House of Representatives, Federal Bureau of Investigation (FBI) Director James Comey characterized the evolving terrorist threat to the Homeland through the successful use of

[7] Richard Burr, "The Debate Over Encryption: Stopping Terrorists From 'Going Dark," *The Wall Street Journal*, December 23, 2015, accessed March 9, 2016, http://www.wsj.com/articles/stopping-terrorists-from-going-dark-1450914378.

[8] "WhatsApp Encryption Shouldn't Be a Safe Haven to Cyber Criminals," *Hindustan Times*, April 7, 2016, accessed April 8, 2016, http://www.hindustantimes.com/tech/whatsapp-encryption-shouldn-t-be-a-safe-haven-to-cyber-criminals/story-M1yBitHmkinvBdpaAhISgI.html.

[9] Evan Perez, "First on CNN: Paris Attackers Likely Used Encrypted Apps, Officials Say," *CNN*, December 17, 2015, accessed March 13, 2016, http://www.cnn.com/2015/12/17/politics/paris-attacks-terrorists-encryption/.

the internet by the Islamic State of Iraq and the Levant (ISIL), also known as ISIS:

> ISIL has used ubiquitous social media to break the model and push into the United States, into the pockets, onto the mobile devices of troubled souls throughout our country in all 50 states a twin message: Come or kill, come or kill. Come to the so-called caliphate, live a life of glory, participate in the final battle between good and evil on God's side. Come to the caliphate, and if you can't come, kill where you are.[10]

In March 2016, the House Homeland Security Committee released a report entitled, "#Terror Gone Viral: Overview of the 75 ISIS-Linked Plots against the West 2014-2016."[11] Among the key findings from the report were that the United States was the favorite target for ISIL-linked plots, followed by France and the United Kingdom. In addition, the number of attacks were increasing as the years went by, and becoming deadlier on average, with a higher death toll with each attack.[12] According to the report, ISIL had successfully "crowd-sourced" its terrorism agenda by inspiring their adherents to conduct most of its attacks: two-thirds of the Islamic State plots against the West appeared to have been "inspired" rather than directed from the top or carried out by trained jihadists.[13]

---

[10] "#Terror Gone Viral: Overview of the 75 ISIS-Linked Plots Against the West 2014-2016," *House Homeland Security Committee*, March 2016, accessed March 9, 2016, https://homeland.house.gov/wp-content/uploads/2016/03/Report-Terror-Gone-Viral-1.pdf.

[11] Ibid.

[12] Ibid.

[13] Ibid.

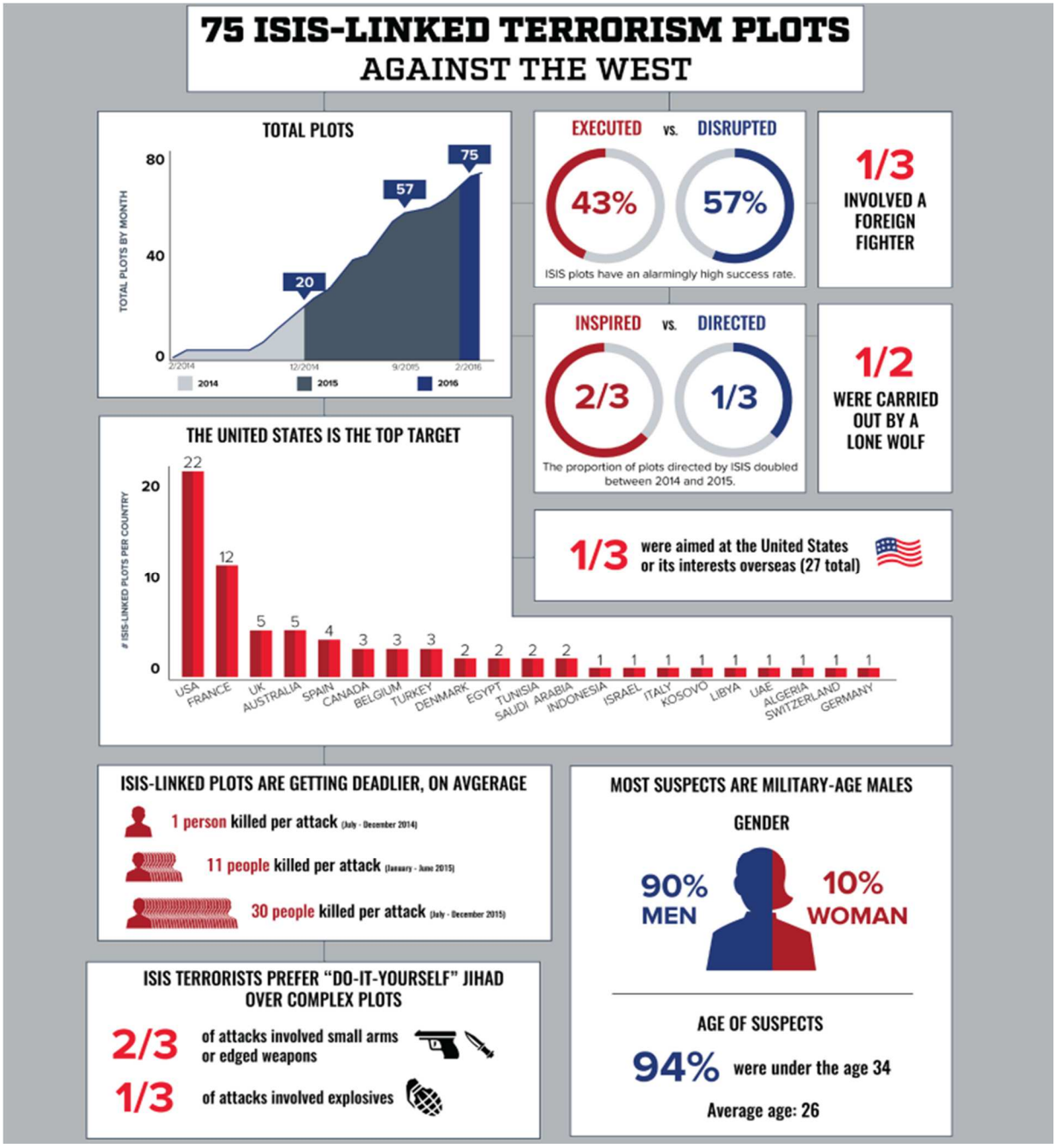
Finally, the report noted that terrorists were "going dark," making it harder in some cases to prevent attacks.[14] Islamic State is pushing out guidance on how to secure their communications, which appeared to be having an effect, as shown by several prominent attacks where terrorists encrypted their communications, making their data inaccessible to authorities, including the attacks in Garland, Texas and Paris, France.[15] In Garland, the suspect reportedly exchanged 109 encrypted messages with a known terrorist overseas before his attack, and in Paris, the attackers allegedly used encrypted communications to plan their operation.[16] In both cases authorities were apparently unable to intercept the messages ahead of time, and that inability to access the information due to encryption has hindered investigations.[17] The following diagram from the Homeland Security report highlights several of the key findings.

[14] Ibid.

[15] Richard Burr, "The Debate Over Encryption: Stopping Terrorists From 'Going Dark'," *The Wall Street Journal*, December 23, 2015, accessed March 9, 2016, http://www.wsj.com/articles/stopping-terrorists-from-going-dark-1450914378.

[16] "#Terror Gone Viral: Overview of the 75 ISIS-Linked Plots Against the West 2014-2016," *House Homeland Security Committee*, March 2016, accessed March 9, 2016, https://homeland.house.gov/wp-content/uploads/2016/03/Report-Terror-Gone-Viral-1.pdf.

[17] Ibid.



As a growing body of research shows, "successful" terrorist attacks are increasingly linked to, and perhaps dependent on, the use of the Internet and secure communications

platforms.[18] As a result of this trend, those who investigate and monitor terrorist threats are focused on the significant investigative hurdles erected by encryption.

At the other end of the spectrum, however, privacy advocates and the technology sector emphasize the virtues of encryption and caution against the degrading effect of an omniscient government and absolute surveillance on a democracy.[19] They argue that encryption has the ability to safeguard privacy, thwart hackers and identity thieves, protect commercial interests and allow for freedom for dissidents to speak freely, as was seen during the Arab Spring in 2011.[2021] A poll of the American people showed that they too were concerned about potential excesses in US government surveillance.[22] In March 2015, the Pew Research Center released a report titled, "Americans' Privacy Strategies Post-Snowden," which attempted to ascertain Americans' thoughts on US government intelligence programs, including the bulk telephone metadata capture that came to light after many of the Edward Snowden documents were released to the public.[23] The survey

---

[18] Ibid.

[19] Eleanor Saitta. "Can Encryption Save Us?" *Nation* 300, no. 24 (June 15, 2015): 16-18. *Academic Search Premier*, EBSCO*host* (accessed February 29, 2016).

[20] Suni Munshani, "The Arab Spring of Privacy is Upon Us," *Wired*, November 7, 2014, accessed March 9, 2016, http://www.wired.com/insights/2014/11/arab-spring-of-privacy/.

[21] Foster Kramer, "Twitter Buys Mobile Encryption Software, Weirdly Pulls It From Market, Basically Hates Egypt," *Observer*, November 11, 2011, accessed March 6, 2016, http://observer.com/2011/11/twitter-buys-mobile-encryption-software-weirdly-pulls-it-from-market-basically-hates-egypt/.

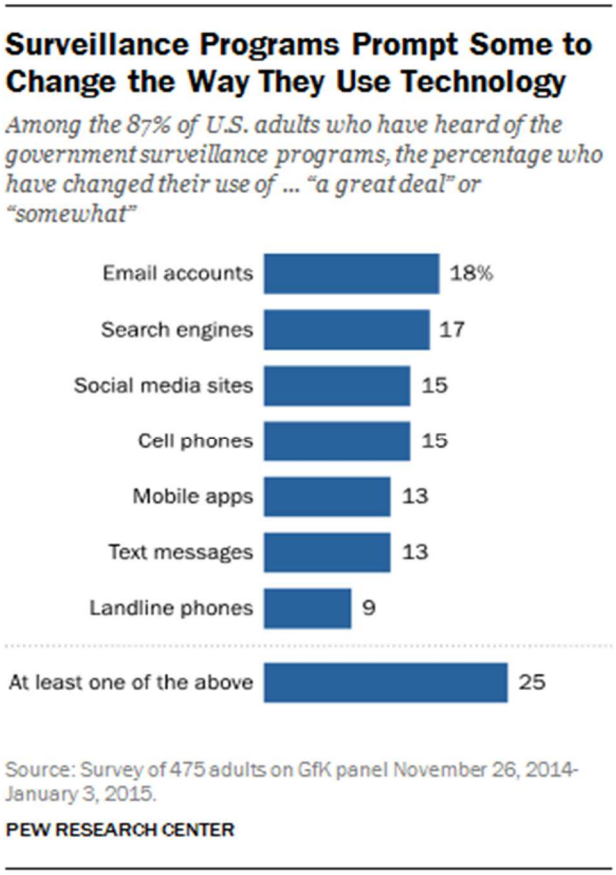
[22] Mary Madden, "Americans' Privacy Strategies Post-Snowden," *Pew Research Center*, March 16, 2015, accessed March 4, 2016, http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/.

[23] Ibid.

asked a sample of American adults what they thought of these government programs, including how the programs were managed and monitored, and whether they personally have altered their communication habits and online activities since learning about the details of these programs.[24] In a demonstration of the strength of the privacy reaction, almost 90% of Americans surveyed indicated they had heard something about the government surveillance program, and 25% of those who were aware of the surveillance programs indicated they had changed their patterns of use of the following technologies

[24] Ibid.

either "a great deal" or "somewhat" since the Snowden revelations:[25]



Therefore, this paper will attempt to navigate between the two extremes of perfect security and perfect privacy, focusing on the role of encrypted messaging applications or "apps" in terrorist plotting and the resulting tensions between the government's mission to protect the nation, and various advocacy groups' desire to preserve the liberties and information security of the individual. The government's ability to maintain the

[25] Ibid.

increasingly delicate balance between liberty and security in an age of rapid technological advances and evolving terrorist threats is an important topic with critical ethical implications. While encryption can empower terrorists in a way that threatens the physical safety of the body politic in a democratic society, unfettered government surveillance can threaten its soul.

After providing an overview of secure messaging through encryption, this paper will examine several case studies that exemplify the terrorist threat vis-à-vis encrypted messaging, and will look at some of the most popular encrypted apps utilized by ISIL to include Wickr, and Telegram. This paper will then examine the case for enhanced privacy and the effects of mass surveillance, and current legislative efforts underway to address the issues raised by both sides. Finally, this paper will conclude with recommendations that can help address the primary concerns voiced by privacy advocates and the technology sector to protect civil liberties while providing meaningful compliance with valid court orders for information on known terrorists that can help prevent future attacks.[26] While neither side may be satisfied with all the recommendations, it is at least a step forward towards a common solution instead of the winner-take-all approaches that are currently being advocated by both sides.

[26] Reema Shah. "Law Enforcement and Data Privacy: A Forward-Looking Approach." *Yale Law Journal* 125, no. 2 (November 2015): 543-558. *Academic Search Premier*, EBSCO*host*, accessed February 28, 2016.

CHAPTER 2

SECURE MESSAGING

To better understand secure messaging, it is important to first understand how messaging has evolved on the mobile phone platform. Currently, over 68% of Americans own a smartphone.[1] Smartphones are differentiated from regular mobile phones by their ability to function as a computer. A smartphone is defined as a mobile phone that performs many of the functions of a computer, typically having a touchscreen interface, Internet access, and an operating system capable of running downloaded applications.[2] Whether or not a smartphone, most mobile phones share the ability to send messages to other mobile phones using a method called text messaging or Short Message Service (SMS).[3] It was a standard communication platform built for the early days of mobile communication, which involved communicating via buttons on a dial pad.[4] Messages were capped in length at 160 characters—a limitation that remains in effect today, although a modern text messaging applications or "apps" will turn longer messages into an MMS (Multimedia Messaging) in order to work around that limitation.[5]

---

[1] Michelle Atkinson, "Apps Permissions in the Google Play Store," *Pew Research Center*, November 10, 2015, accessed March 4, 2016, http://www.pewinternet.org/files/2015/11/PI_2015-11-10_apps-permissions_FINAL.pdf.

[2] "Smartphone," *Oxforddictionaries.com*, accessed March 4, 2016, http://www.oxforddictionaries.com/us/definition/american_english/smartphone.

[3] Derek Walter, "Why You Should Ditch SMS and Embrace Over-the-Top Messaging Apps," *Green Bot*, July 20, 2015, accessed March 4, 2015, http://www.greenbot.com/article/2948898/android-apps/why-you-should-ditch-sms-and-embrace-over-the-top-messaging-apps.html.

[4] Ibid.

[5] Ibid.

Instant messaging works much differently than SMS or MMS text messaging. Messages are sent over the Internet and through the servers of whichever company runs the messaging service.[6] As such, an individual only needs an Internet connection to communicate, whereas with SMS, the individual's device needs to be connected to a cellular network. [7] Because smartphones function like computers, they are able to run Instant Messaging (IM) programs or apps.[8] These mobile messaging apps are frequently called "over-the-top" (OTT) messaging, as the services operate on the Internet as an alternative to what is offered by the phone carrier.[9] However, most mobile messaging apps are not secure.[1011] After the Snowden revelations revealed that mobile phones were being exploited by the US Government, an effort to secure mobile communications emerged.[12] A flood of new messaging apps were introduced that combined the ease and

[6] Ibid.

[7] Ibid.

[8] Ibid.

[9] Ibid.

[10] Dell Cameron, "Edward Snowden Tells You What Encrypted Messaging Apps You Should Use," *The Daily Dot*, March 6, 2015, accessed March 7, 2016, http://www.dailydot.com/politics/edward-snowden-signal-encryption-privacy-messaging/.

[11] "Secure Messaging Scorecard," *Electronic Frontier Foundation*, November 11, 2014, accessed March 4, 2016, https://www.eff.org/secure-messaging-scorecard#about.

[12] Stephanie Mlot, "Only 6 Messaging Apps Are Truly Secure," *PC Magazine*, November 5, 2014, accessed March 5, 2016, http://www.pcmag.com/article2/0,2817,2471658,00.asp.

speed of instant messaging, with the security of encryption. These apps are referred to as encrypted messaging apps.[13]

Encryption is defined as the process of converting information or data into a code, especially to prevent unauthorized access.[14] Edward Snowden warns that on mobile devices, messages in transit are the easiest to intercept .[15] Therefore, he argues the "only way to protect messages from being intercepted by malicious third-parties, is to communicate using a service that provides end-to-end encryption."[16] There are many encrypted messaging apps available today on mobile smart phones.[17] Each of these communications apps has their own unique interface, capabilities and security features.[18] Also, each is unique to the technology ecosystem of the user—that is, whether the user has an Android, Windows or iOS smartphone.

In August 2015, the Pew Research Center conducted a survey specifically on mobile messaging apps and their popularity among young adults. The survey discovered

---

[13] Esther Shein. "Ephemeral Data." *Communications Of The ACM* 56, no. 9 (September 2013): 20-22. *Academic Search Premier*, EBSCO*host*, accessed March 8, 2016.

[14] "Encryption," *Oxforddictionaries.com*, accessed March 7, 2016. http://www.oxforddictionaries.com/us/definition/american_english/encryption.

[15] Dell Cameron, "Edward Snowden Tells You What Encrypted Messaging Apps You Should Use," *The Daily Dot*, March 6, 2015, accessed March 7, 2016, http://www.dailydot.com/politics/edward-snowden-signal-encryption-privacy-messaging/.

[16] Ibid.

[17] "Secure Messaging Scorecard," *Electronic Frontier Foundation*, November 11, 2014, accessed March 4, 2016, https://www.eff.org/secure-messaging-scorecard#about.

[18] KeriLynn Engel, "True Private Messaging: 7 Apps to Encrypt Your Chats," *WhoIsHostingThis Blog*, April 29, 2015, accessed March 5, 2016, http://www.whoishostingthis.com/blog/2015/04/29/im-encryption/.

that 36% of smartphone owners use or own at least one messaging app, and that 17% use messaging apps that auto-delete their information.[19] When focusing on the 18 to 29 year-old demographic, the use of messaging apps, and encrypted messaging apps in particular, goes up by a much larger percentage.[20] Almost half (49%) of smartphone owners surveyed ages 18 to 29 use messaging apps, and 41% of that same demographic utilize auto-delete messaging applications such as Snapchat and Wickr.[21]

[19] Maeve Duggan, "Mobile Messaging and Social Media 2015," *Pew Research Center*, August 19, 2015, accessed March 4, 2016, http://www.pewinternet.org/files/2015/08/Social-Media-Update-2015-FINAL2.pdf.

[20] Ibid.

[21] Ibid.

Mobile Messaging Apps Particularly Popular Among Young Adults

Among smartphone owners, the % who use messaging apps and apps that automatically delete sent messages

	Messaging apps	Auto-delete apps
Total	*36%*	*17%*
Men	37	17
Women	36	18
White, Non-Hispanic	34	18
Black, Non-Hispanic	N/A*	N/A*
Hispanic	N/A*	N/A*
18-29	49	41
30-49	37	11
50+	24	4
High school grad or less	30	19
Some college	34	20
College+	45	13
Less than $50,000/yr	37	18
$50,000+	36	17
Urban	42	22
Suburban	37	15
Rural (n=99 smartphone owners)	22	13

Source: Pew Research Center, March 17-April 12, 2015.

* Because some questions were given to half the respondents, there are not enough cases to allow sufficient statistical analysis for these groups.

PEW RESEARCH CENTER

Although many users had previously felt their information was protected through the use of public key encryption systems, the Snowden leaks revealed that government surveillance against so-called encrypted systems was still widespread.[22] In June 2013, the United Kingdom-based newspaper, *The Guardian*, published a document leaked by Edward Snowden wherein the US National Security Agency (NSA) claimed they had

[22] James Ball, "Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security," *The Guardian*, September 6, 2013, accessed March 7, 2016, http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

"direct access" to the networks of technology giants Apple, Google, Microsoft and Facebook through its PRISM program.[23] It was also revealed that Microsoft was complicit in providing the NSA with access to its systems and networks, even going so far as to provide the agency with its encryption keys.[24] These and other leaked documents illustrated the scale of cooperation between Silicon Valley and the US intelligence agencies over a three-year period, and shed new light on the workings of the top secret PRISM program.[25] In addition, the documents also highlighted that Microsoft helped the NSA circumvent Microsoft's encryption to address the agency's concerns that it would be unable to intercept web chats on the new Outlook.com portal, and revealed that he agency already had pre-encryption access to email on Outlook.com and Hotmail.com.[26]

In defense of its actions, Microsoft issued a statement that when it upgrades or updates its products, the company is not "absolved from the need to comply with existing or future lawful demands."[27] The company also pointed out that it provided user information or data only in response to government orders, and only regarding specific

[23] Glenn Greenwald, "NSA Prism Program Taps in to User Data of Apple, Google, and Others," *The Guardian*, June 7, 2013, accessed March 7, 2013, http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

[24] Glenn Greenwald, "Microsoft Handed the NSA Access to Encrypted Messages," *The Guardian*, July 12, 2013, accessed March 12, 2016, http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data.

[25] Ibid.

[26] Ibid.

[27] Ibid.

accounts or identifiers.[28] Soon after the Snowden revelations, many tech companies began to distance themselves from the Government while voicing their frustrations to the White House.[29] In a December 9, 2013 letter to President Obama, leaders from US technology companies Yahoo, Google, Facebook, Apple, Microsoft, Twitter, LinkedIn and AOL recommended that the President rein in the NSA and allow the companies to alert users to what data the government is seeking from the companies.[30] In addition, each company listed above with the exception of AOL, took part in a roundtable discussion with the White House to discuss fallout from the NSA disclosures.[31] In June 2013, Google requested from the Department of Justice the ability to reveal to the American public "what data the government is seeking from them."[3233] In 2014, Twitter sued the US government for the ability to tell its users about national security requests it receives from the government.[34]

---

[28] Ibid.

[29] Margaret Talev,"NSA Fallout Tests Obama Relationship With Tech Companies," *Bloomberg*, December 18, 2013, accessed March 12, 2016,http://www.bloomberg.com/news/articles/2013-12-18/nsa-fallout-tests-obama-relationship-with-tech-companies.

[30] Ibid.

[31] Ibid.

[32] Ibid.

[33] Sam Gustin, "Google: We're No NSA Stooge and We'll Prove It if the Feds Let Us," *Time,* June 11, 2013, accessed March 12, 2016, http://business.time.com/2013/06/11/google-were-no-nsa-stooge-and-well-prove-it-if-the-feds-let-us/.

[34] Ellen Nakashima, "Twitter Sues U.S. Government Over Limits on Ability to Disclose Surveillance Orders," *The Washington Post,* October 7, 2014, accessed March 13, 2016, https://www.washingtonpost.com/world/national-security/twitter-sues-us-government-over-limits-on-ability-to-disclose-surveillance-orders/2014/10/07/5cc39ba0-4dd4-11e4-babe-e91da079cb8a_story.html.

Tech companies have very good reasons to distance themselves from the NSA disclosures.[35] Mass surveillance programs are extremely unpopular with the American public, and undermined users' confidence in these tech companies at home and abroad.[36] Tech companies worried that if customers began to feel that their information was not safe, they might take their business elsewhere, depriving the company of valuable revenue.[37] Indeed, according to a March 2014 article in *The New York Times* entitled, "Revelations of N.S.A. Spying Cost U.S. Tech Companies," Microsoft had lost technology accounts from the country of Brazil due to the Snowden revelations.[38] In addition, the article detailed how companies offering cloud computing services would also be affected by the NSA scandal. According to a report by the Information Technology & Innovation Foundation (ITIF), US cloud computing companies stand to

[35] Margaret Talev, "NSA Fallout Tests Obama Relationship With Tech Companies," *Bloomberg*, December 18, 2013, March 12, 2016, http://www.bloomberg.com/news/articles/2013-12-18/nsa-fallout-tests-obama-relationship-with-tech-companies.

[36] Mary Madden, "Americans' Attitudes About Privacy, Security and Surveillance," *Pew Research Center*, May 20, 2015, March 11, 2016, http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

[37] Margaret Talev, "NSA Fallout Tests Obama Relationship With Tech Companies," *Bloomberg*, December 18, 2016, March 12, 2016, http://www.bloomberg.com/news/articles/2013-12-18/nsa-fallout-tests-obama-relationship-with-tech-companies.

[38] Claire Cain Miller, "Revelations of N.S.A Spying Cost U.S. Tech Companies, *The New York Times*, March 22, 2014, March 9, 2016, http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html?_r=1.

lose up to $35 Billion by 2016 due to the NSA PRISM program.[39] Others calculated potential losses as high as $180 billion, or 25% of overall revenue.[40]

In addition to financial considerations, tech companies were further motivated to distance themselves from the US government from information indicating the US government had surveillance programs targeting their networks without their knowledge, and that the government had gained access to their systems without a court order[41]. For instance, Google and Yahoo were unaware that their server data centers around the world had been compromised by the NSA.[42] Mike Hearn, a security engineer at Google, addressed one of the released documents which demonstrated how the NSA had gotten access to Google's data center.[43]

---

[39] Ibid.

[40] James Staten, "The Cost of PRISM Will Be Larger Than ITIF Projects," *Forrester Research: James Staten's Blog*, August 14, 2013, accessed March 9, 2016, http://blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects.

[41] Glenn Greenwald, NSA Prism Program Taps in to User Data of Apple, Google, and Others," *The Guardian*, June 7, 2013, accessed March 7, 2013, http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

[42] Barton Gellman, "How We Know The NSA Had Access to Internal Google and Yahoo Cloud Data," *The Washington Post*, November 4, 2013, March 9, 2016, https://www.washingtonpost.com/news/the-switch/wp/2013/11/04/how-we-know-the-nsa-had-access-to-internal-google-and-yahoo-cloud-data/.

[43] Mike Masnick, "Pissed Off Google Security Guys Issue FU To NSA, Announce Data Center Traffic Now Encrypted," *TechDirt*, November 6, 2013, accessed March 12, 2016, https://www.techdirt.com/articles/20131106/00235225143/pissed-off-google-security-guys-issue-fu-to-nsa-announce-data-center-traffic-now-encrypted.shtml.

In a post on his Google+ account, Mike Hearn stated:

> We designed this system to **keep criminals out**. There's no ambiguity here. The warrant system with skeptical judges, paths for appeal, and rules of evidence was built from centuries of hard won experience. When it works, it represents as good a balance as we've got between the need to restrain the state and the need to keep crime in check. Bypassing that system **is illegal for a good reason**. Unfortunately, we live in a world where all too often, laws are for the little people. Nobody at GCHQ or the NSA will ever stand before a judge and answer for this industrial-scale subversion of the judicial process. In the absence of working law enforcement, we therefore do what internet engineers have always done - build more secure software. The traffic shown in the slides below is now all encrypted and the work the NSA/GCHQ staff did on understanding it, ruined. Thank you Edward Snowden. For me personally, this is the most interesting revelation all summer.[44]

The NSA surveillance scandal spurred the introduction of forward secrecy, which is an encryption scheme whereby new encryption keys are generated with each chat session.[45] With forward secrecy, unlike with earlier encryption schemes, if an unwanted third party somehow stole the encryption key in a chat session between two individuals, the third party would be only able to decipher the messages from the one session, but would not be able to read messages from any other session.[46] On November 22, 2013,

---

[44] Ibid.

[45] Hal Abelson, "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption," *MIT Computer Science and Artificial Intelligence Laboratory*, May 27, 1997, accessed March 14, 2016, https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/key-study-report.html.

[46] Richard Mortier, “Explainer: What is Perfect Forward Secrecy,” *The Conversation*, December 2, 2013, accessed March 2, 2016, http://theconversation.com/explainer-what-is-perfect-forward-secrecy-20863.

Twitter announced the implementation of perfect forward secrecy across its platform.[47] In a written statement, Twitter announced that it enabled forward secrecy for traffic on twitter.com, api.twitter.com, and mobile.twitter.com as "part of [their] continuing effort to keep [] users' information as secure as possible."[48] On top of the usual confidentiality and integrity properties of HTTPS, Twitter's perfect forward secrecy ensures that if an adversary were recording all Twitter users' encrypted traffic, and they later crack or steal Twitter's private keys, they would not be able to use those keys to decrypt the recorded traffic.[49]

According to the Electronic Frontier Foundation (EFF), a non-profit organization with the stated mission to defend civil liberties in the digital realm, the type of protection provided by encryption is critical in securing a users privacy.[5051] In 2015, the EFF issued a report called the "Secure Messaging Scorecard," which evaluated 39 secure messaging services based on 7 metrics of proven security measures.[52] The EFF argued that the

[47] Jacob Hoffman-Andrews, "Forward Secrecy at Twitter," *The Twitter Engineering Blog*, November 22, 2013, accessed March 2, 2016, https://blog.twitter.com/2013/forward-secrecy-at-twitter-0.

[48] Ibid.

[49] Ibid.

[50] "About EFF," *Electronic Frontier Foundation*, accessed March 4, 2016, https://www.eff.org/about.

[51] "Secure Messaging Scorecard," *Electronic Frontier Foundation*, November 11, 2014, accessed March 4, 2016, https://www.eff.org/secure-messaging-scorecard#about.

[52] Ibid.

"Snowden revelations have confirmed our worst fears: governments are spying on our digital lives, grabbing up communications transmitted in the clear."[53]

Despite popular discontent over widespread government surveillance, encryption tools are still not routinely and extensively used by the general public, possibly due to two things: security and usability.[54] Most of the tools that are user-friendly for the general public are often not secure.[55] Messaging tools that are really secure are often not user-friendly, and everyday users may have trouble installing the technology and correctly applying the appropriate encryption settings.[56] One report stated that "users expect software to "just work" without worrying too much about the technical details. But the researchers discovered that users tended to make mistakes that compromise their security."[57] In creating the Secure Messaging Scorecard, the EFF's stated goals "are championing technologies that are strongly secure and also simple to use…These are the tools everyday users need to communicate with friends, family members, and colleagues, and we need secure solutions for them."[58] In addition, the hope of the EFF was that the

[53] Ibid.

[54] Ibid.

[55] Ibid.

[56] Timothy Lee, "NSA-Proof Encryption Exists. Why Doesn't Anyone Use It?," *The Washington Post*, June 14, 2013, accessed March 8, 2016, https://www.washingtonpost.com/news/wonk/wp/2013/06/14/nsa-proof-encryption-exists-why-doesnt-anyone-use-it/.

[57] Ibid.

[58] "Secure Messaging Scorecard," *Electronic Frontier Foundation*, November 11, 2014, accessed March 4, 2016, https://www.eff.org/secure-messaging-scorecard#about.

scorecard might also "serve as a race-to-the-top, spurring innovation around strong crypto for digital communications."[59]

Only 6 encryption apps managed to meet all 7 of the EFF Scorecard's security metrics: ChatSecure + Orbot, Cryptocat, RedPhone, Silent Phone, Silent Text, and TextSecure.[60] Many of the most current popular instant messaging apps such as SnapChat, Skype,

[59] Ibid.

[60] Stephanie Mlot, "Only 6 Messaging Apps Are Truly Secure," *PC Magazine*, November 5, 2014, accessed March 5, 2016, http://www.pcmag.com/article2/0,2817,2471658,00.asp.

Facebook and Google Hangouts only met two of the EFF's criteria, while AOL Instant Messenger fared the worst, satisfying one of the seven criteria for secure messaging.[61]

When it comes to concerns over secure communications, ISIL, for its part, has also weighed in on the importance of secure messaging and has become one of its most ardent--and nefarious-- supporters.[62] The group has built a tech-savvy division of commanders who issue tutorials to its sympathizers instructing on the most secure and least expensive ways of communicating.[63] After the Paris Attacks in November 2015, *The Wall Street Journal* published an article entitled, "How Islamic State Teaches Tech Savvy To Evade Detection," documenting how ISIL is the furthest along among terrorist organizations in promoting social media and encrypted messaging technology through the use of online tutorials, videos and even recommendations to their online followers on which types of mobile phone hardware to purchase.[64] In January 2015, ISIL supporter known online as "al-Khabir al-Taqni" (al-Taqni), a self-identified "technical expert," provided would-be ISIL fighters with a list of what he determined were the safest

[61] "Secure Messaging Scorecard," *Electronic Frontier Foundation*, November 11, 2014, accessed March 4, 2016, https://www.eff.org/secure-messaging-scorecard#about.

[62] Istvan Fekete, "iMessage Ranked 'Moderately Safe' by Islamic State, Telegram Preferred," *iPhone in Canada*, November 18, 2015, accessed March 11, 2016, http://www.iphoneincanada.ca/news/imessage-ranked-moderately-safe/.

[63] Margaret Coker, "How Islamic State Teaches Tech Savvy to Evade Detection," *Wall Street Journal (Online)*, November 17, 2015., 1, *Academic Search Premier*, EBSCO*host*, accessed April 14, 2016.

[64] Ibid.

encrypted communications systems available.[65] Al-Taqni emphasized the importance of utilizing such technology, stating that "[t]hrough this, we can break one of the strongest weapons of the Crusader governments in spying on and tracking the mujahedeen and targeting them with aircraft," referring to the US-led coalition fighting ISIL.[66]

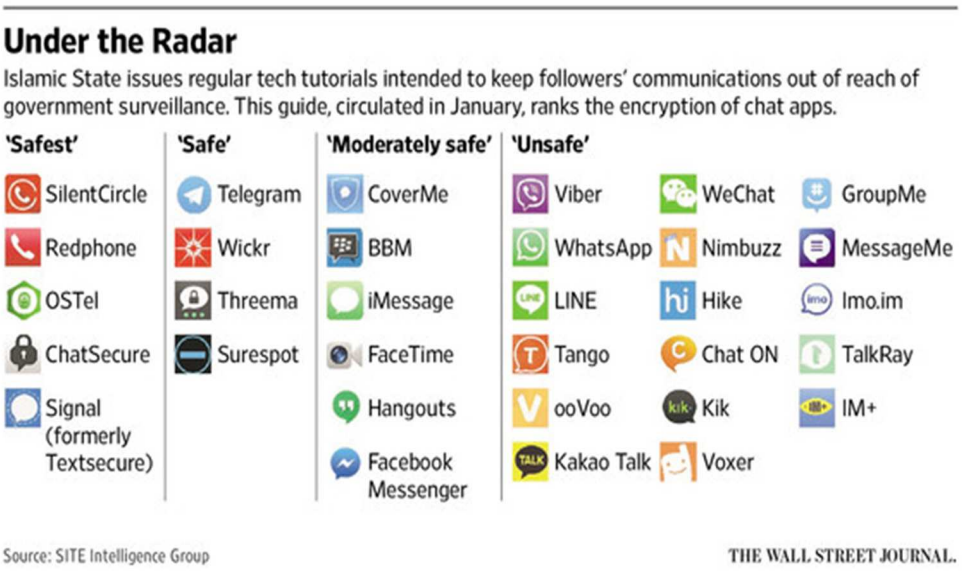
Al-Taqni, similar to the EFF, ranked 33 secure messaging applications, according to the SITE Intelligence Group, which closely monitors the online activities of terrorist groups worldwide.[67] Al-Taqni ranked the various encrypted applications as unsafe, moderately safe, safe and safest.[68] There was some overlap between Al-Taqni's and EFF's ratings, with some of the "safest" applications being SilentCircle (also known as SilentPhone), Redphone, ChatSecure+ and TextSecure (now known as Signal).

[65] Ibid.

[66] Ibid.

[67] Ibid.

[68] Ibid.



In remarks before an open session of the Senate Select Committee on Intelligence on July 7, 2015, FBI Director James Comey explained to committee members that ISIL-- to an even greater degree than al Qaeda or other foreign terrorist organizations-- has persistently used the Internet to communicate, and has aggressively employed this technology for its nefarious strategy.[69] Comey stated that from a homeland perspective, ISIL's widespread reach through the Internet and social media is most concerning, as social media has allowed groups such as ISIL to use the Internet to spot and assess potential recruits.[70] According to Comey, [w]ith the widespread horizontal distribution of social media, terrorists can identify vulnerable individuals of all ages in the United

[69] US Congress, Senate, *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy: Hearing before the Committee on the Judiciary*, 114th Cong., 1st sess., July 08, 2015, (statement of James B. Comey, Director, Federal Bureau of Investigation).

[70] Ibid.

States—spot, assess, recruit, and radicalize— either to travel or to conduct a homeland attack. The foreign terrorist now has direct access into the United States like never before.[71]

Director Comey further explained that during the month preceding the 2015 Independence Day holiday in the United States, the FBI had over a hundred active investigations in all 50 states.[72] Comey also testified before the Senate regarding the growing trend of "going dark" or, as he characterized it, the growing divide between the government having lawful court orders for information and technology making the information undecipherable or unavailable.[73] He referenced the use of encrypted applications that rode on the backbone of the Internet, and gave an example of the intersection between social media and encrypted applications, specifically the use of Twitter by ISIL operatives in Syria to reach out to, and initiate contact with, individuals in the West, including the United States.[74] After establishing contact using open communications on social media platforms such as Twitter, ISIL operatives would then instruct individuals to utilize an encrypted app in order to engage in further dialogue away from the prying eyes of the government. Once the discussions moved to encrypted

[71] Ibid.

[72] Ibid.

[73] Ibid.

[74] Ibid.

platforms, neither the FBI nor the rest of the USIC could see the contents of the communications.[75]

Director Comey stated that it was not his intention to frighten, but to begin an earnest conversation on how privacy could be protected while still preserving the government's ability to execute valid court orders under the 4th Amendment of the U.S. Constitution.[76] Acknowledging that although there might not be a "right answer" to the problem, Director Comey argued that Silicon Valley technology companies and the government still needed to work together in order to ascertain if a new framework could be implemented that preserved access while protecting privacy.[77]

[75] Ibid.

[76] Ibid.

[77] Ibid.

CHAPTER 3

JUNAID HUSSAIN

Junaid Hussain, also known as Abu Hussain al-Britani, was a United Kingdom (UK) resident and the eventual head of the CyberCaliphate, ISIL's cyber warfare arm.[1] He came to embody the worst fears of the law enforcement and intelligence communities and represented a new generation of terrorists and their abilities in the social media and communications landscape.[2] Hussain was born in Birmingham, England and was a gifted student with computers.[3] Hussain had received offers from two universities in the UK to study computer forensics, but instead turned his attention and skills towards aiding the global jihadist movement.[4] Hussain first came to prominence in the UK in 2012 after he hacked the e-mail account of British Prime Minister Tony Blair and his key advisor Katy Kay, exposing over 150 contacts of the Prime Minister along with his personal email

[1] "I.S. Plot to Bomb UK Today," *The Sun*, June 26, 2015, accessed March 7, 2016, http://www.thesun.co.uk/sol/homepage/news/6518366/Islamic-State-monster-aimed-to-kill-British-soldiers.html.

[2] Meg King, "Opinion: The Shocking Mediocrity of Islamic State 'Hacker' Junaid Hussain," *The Christian Science Monitor*, October 26, 2015, accessed March 8, 2016, http://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/1026/Opinion-The-shocking-mediocrity-of-Islamic-State-hacker-Junaid-Hussain.

[2] Ibid.

[3] Gianluca Mezzofiore, "Team Poison's Junaid Hussain Jailed for Tony Blair Hack and Phone Bombing Anti-Terror Hotline," *International Business Times*, July 27, 2013, accessed March 8, 2016, http://www.ibtimes.co.uk/team-poison-phone-bomb-hacker-anti-terror-367660.

[4] "I.S. Plot to Bomb UK Today," *The Sun*, June 26, 2015, accessed March 7, 2016, http://www.thesun.co.uk/sol/homepage/news/6518366/Islamic-State-monster-aimed-to-kill-British-soldiers.html.

account.[5] Hussain was found, captured and jailed for 6 months for this cyber attack.[6] Upon being granted bail, Hussain fled Birmingham, UK to join ISIL in Syria, where he eventually became the head of the CyberCaliphate.[7] In this role, Hussain led a hacking attack against the United States Central Command (USCENTCOM) Twitter account, briefly overtaking the account over and posting pro-ISIL messages favorable to ISIL.[8]

Abu Hussain al-Britani set out creating a team that would eventually leverage social media and encrypted communication mobile apps to identify, recruit and direct operations against western targets.[9] In April 2015, the Stop Islamization of America group, also known as the American Freedom Defense Initiative (AFDI), planned a Stand Up for the Prophet Event, specifically a "Draw Mohammad" contest, to be held at the Curtis Culwell Center in Garland, Texas.[10] Both the group and the event were highly controversial. SIOA claims to be a civil liberties advocacy group, but other organizations

[5] Ibid.

[6] Ibid.

[7] Ibid.

[8] Spencer Ackerman, "Junaid Hussain: British Hacker for ISIS Believed Killed in US Air Strike," *The Guardian*, August 27, 2015, accessed March 7, 2016, http://www.theguardian.com/world/2015/aug/27/junaid-hussain-british-hacker-for-isis-believed-killed-in-us-airstrike.

[9] "I.S. Plot to Bomb UK Today," *The Sun*, June 26, 2015, accessed March 7, 2016, http://www.thesun.co.uk/sol/homepage/news/6518366/Islamic-State-monster-aimed-to-kill-British-soldiers.html.

[10] Letitia Stein, "Mohammad Cartoonist Says Police Killing of Two Gunmen 'Justice'," *Reuters*, May 4, 2015, accessed March 7, 2016, http://www.reuters.com/article/us-usa-shooting-texas-cartoonist-idUSKBN0NP1ZS20150504.

such as the Southern Poverty Law Center (SPLC) categorizes them as a "hate group."[11] The SIOA, led by Pamela Geller, counters the notion by stating that she established the event as a "political critique" of Islam.[12] She further went on to state that "We absolutely must have other events like this to stand up for free speech...I will not abridge my freedoms so as not to offend savages."[13]

Security around the event was tight that night due to the controversial subject matter, but also because of the appearance of guest speaker Geert Wilders, a Dutch politician who is reviled across the Islamic world for his views on Islam.[14] Organizers of the event stated that they had spent over $10,000 on security and hired over 40 security guards.[15] A little before 7 pm PST, Elton Simpson posted on Twitter: "May Allah accept us as mujahedeen," with the hashtag the hashtag #texasattack .[16] In his tweet, he said he and an accomplice had pledged allegiance to "Amirul Mu'mineen," which was likely a

[11] Ibid.

[12] William J. Gorta, "Garland Shooting: 'Draw Muhammad' Contest Host Pamela Geller Wants More, Similar Events," *NBC News*, May 5, 2015, accessed March 8, 2016, http://www.nbcnews.com/news/us-news/host-draw-muhammad-contest-says-must-be-more-similar-events-n353546.

[13] Ibid.

[14] Jon Queally, "Anti-Muslim Event in Texas Ends in Gunfire, Two Deaths," *Common Dreams*, May 4, 2015, accessed March 8, 2016, http://www.commondreams.org/news/2015/05/04/anti-muslim-event-texas-ends-gunfire-two-deaths.

[15] Ibid.

[16] Holly Yan, "Texas Attack: What We Know About Elton Simpson and Nadir Soofi," *CNN*, May 5, 2015, accessed March 7, 2016, http://www.cnn.com/2015/05/05/us/texas-shooting-gunmen.

reference to ISIL leader Abu Bakr al-Baghdadi.[17] The user also asked his readers to follow Junaid Hussain on Twitter.[18]

Around 7 pm PST, close to the end of the event, violence erupted. Two men, Elton Simpson and Nadir Hamid Soofi, who traveled from Phoenix, Arizona to Garland, Texas arrived with several assault rifles, multiple handguns and 1,500 rounds of ammunition.[19] Simpson and Soofi opened fire outside the event, wounding a security officer, before being killed by local police.[20]

After the shooting occurred, Hussain tweeted: "Allahu Akbar!!!!! 2 of our brothers just opened fire at the Prophet Muhammad (s.a.w) art exhibition in texas!"[21] ISIL later claimed responsibility for the attack on its official radio station, stating that "two of the soldiers of the caliphate executed an attack on an art exhibit in Garland, Texas, and this exhibit was portraying negative picture of the prophet Mohammad…We tell America that what is coming will be even bigger and more bitter, and that you will

[17] Ibid.

[18] Ibid.

[19] Nigel Duara, "Man Tied to Cartoon Contest Attack Accessed Islamic State List, Authorities Say," *Los Angeles Times*, December 24, 2015, accessed March 8, 2016, http://www.latimes.com/nation/la-na-garland-attack-20151224-story.html.

[20] Ibid.

[21] Robert Spencer, "Allahu Akbar!!!!! 2 of our brothers just opened fire at the Prophet Muhammad (s.a.w) art exhibition in texas!," *Jihad Watch*, May 3, 2015, accessed March 7, 2016, https://www.jihadwatch.org/2015/05/allahu-akbar-2-of-our-brothers-just-opened-fire-at-the-prophet-muhammad-s-a-w-art-exhibition-in-texas.

see the soldiers of Isis do terrible things"[22] The extent of ISIL's involvement in planning or directing the attack has not been confirmed, but if Simpson and Soofi were indeed directed by ISIL, the event would mark the first ISIL attack against the United States on US soil.[23]

Complicating efforts to determine ISIL's involvement in the attacks has been the inability to uncover the communications between the attacker Simpson and presumably Junaid Hussain.[24] In a meeting with Congress in December 2015, FBI Director James Comey stated that on the morning of the attack in Garland, Texas, one of the gunmen exchanged 109 messages with an overseas terrorist.[25] Unfortunately, the FBI had no idea what was said and no way of finding out because the messages were encrypted.[26] At present, there is still no way for law enforcement to access Simpson's encrypted messages, leaving a potential blind spot regarding the specifics of attack plan, who else

[22] Tom Porter, "Texas Shooting: ISIS Claims Responsibility for Attack on Mohammed Cartoons Contest," *International Business Times,* May 5, 2015, accessed March 7, 2016, http://www.ibtimes.co.uk/texas-shooting-isis-claims-responsibility-attack-mohammed-cartoons-contest-1499685.

[23] David E. Sanger, "F.B.I. Chief Says Texas Gunman Used Encryption to Text Overseas Terrorist," *The New York Times*, December 9, 2015, accessed March 9, 2016, http://www.nytimes.com/2015/12/10/us/politics/fbi-chief-says-texas-gunman-used-encryption-to-text-overseas-terrorist.html?_r=0.

[24] Ibid.

[25] Ibid.

[26] Robert Spencer, "Garland Jihadi Sent 109 Encrypted Messages That FBI Can't Read," *Jihad Watch*, December 11, 2015, accessed March 7, 2016, https://www.jihadwatch.org/2015/12/garland-jihadi-sent-109-encrypted-messages-that-fbi-cant-read.

may be involved, or if any other future attacks were discussed.[27] Law Enforcement may never find out if this attack was plotted externally in Syria, or within the United States.

With the success of stoking fear with the Garland attack in May, Hussain may have been ready to turn his focus back against his former homeland, the United Kingdom.[28] On June 1, 2015, Hussain reached out to an individual on the social media messaging app, Kik.[29] Hussain asked the individual if he/she were able to "do something over there," promising an "easy ticket to *jannah* [paradise]."[30] Four days later, the individual responded to Hussain with the message he was "willing to do the work for allah."[31] Hussain, satisfied with that positive response, instructed the individual to move communications from the unsecured Kik social media app to an encrypted communications app called SureSpot.[32] Junaid later reiterated the importance of only using SureSpot because it was secure."[33] Upon entering a secure communication channel with the would-be attacker, Hussain asked the individual where he was from and if he had the ability to get access to weapons

[27] "I.S. Plot to Bomb UK Today," *The Sun*, June 26, 2015, accessed March 7, 2016, http://www.thesun.co.uk/sol/homepage/news/6518366/Islamic-State-monster-aimed-to-kill-British-soldiers.html.

[28] Ibid.

[29] Ibid.

[30] Ibid.

[31] Ibid.

[32] Ibid.

[33] Ibid.

such as handguns and rifles.[34] The would-be attacker replied that he was from London, but stated he was unable to get access to firearms.[35] Hussain responded with "OK perfect. In the heart of the crusader army. We hit them hard."[36] At this point Hussain finally had access to a UK-based individual who could act as an operative to strike at one of his biggest targets in the West, even though the individual could not get a weapon. What Hussain also did not realize was that the would-be attacker was an investigative journalist for the UK-based newspaper, *The Sun*.[37] Revealing his intentions, Hussain told the journalist:

> I can help u inshAllah. We can train you. Plan with u. We can tell you how to make bombs...It will be big. We will hit the kuffar (*unbelievers*) hard InshAllah. Hit their soldiers in their own land. InshAllah. Soldiers that served in Iraq and Afghanistan will be present. Jump in the crowd and detonate the bomb…They think they can kill Muslims in Iraq and Afghanistan then come back to the UK and be safe. We'll hit them hard InshAllah. By Allah you wont be wasted Akhi.[38]

Hussain envisioned the journalist utilizing a pressure cooker bomb similar to the bomb used in the London attacks on July 7, 2005 and the 2013 Boston Marathon bombing.[39] In order to verify the validity of the would-be attacker's intentions, Hussain

---

[34] Ibid.

[35] Ibid.

[36] Ibid.

[37] Ibid.

[38] Ibid.

[39] Ibid.

asked that the individual purchase a pressure cooker and send a photo of it alongside a card with the individuals name on it.[40] After successfully meeting this demand, over the next week he was given a list of household or easily obtainable items to begin constructing the bomb.[41] Hussain then provided, via secure communication channels, a nine-page manual that detailed how exactly to create the bombs from the items previously purchased.[42] The front cover of the document warned: "Keep this document private – do not upload on the internet and do not share with anyone!"[43] Hussain's manual also included instructions on how to inflict maximum destruction and injury, such as by utilizing shrapnel laced with rat poison, in order to prevent blood clotting from even minor wounds.[44]

After the bomb was built, Hussain unveiled the target for the attack: the upcoming Armed Forces Day parade.[45] He asked the would-be attacker: "Akhi can u be ready for the 27th of this month? Its armed forces day. There will be a parade in Woolwich. I'll get you the details."[46] Junaid then instructed the would-be attacker/journalist to create a martyrdom video which would be sent to Hussain securely, and then released upon his

[40] Ibid.

[41] Ibid.

[42] Ibid.

[43] Ibid.

[44] Ibid.

[45] Ibid.

[46] Ibid.

successful bombing operation in order to further strike fear into the population via the media.[47] Hussain also told the journalist how to use the bomb, stating, "U put it in a back pack walk into a crowded area and press the button."[48]

Fortunately, there was no attack on the day of the parade because *The Sun* had already reached out to the UK authorities to warn of the plot, and turned over their communications log and the bomb-making manual.[49] Over 1,000 people attended the parade in 2014, so the potential for casualties was very high.[50] On that day, *The Sun* released its article detailing the thwarted attack along with how Hussain had been tricked by an undercover investigative journalist.[51] Law enforcement officials wondered if similar instructions were passed to Elton Simpson before the Garland, Texas attack, and if they were being passed to others.[52] The 109 encrypted messages to Simpson along with the foiled attempt to attack the Armed Forces Day parade was a wakeup call about the problem of encrypted communications to counterterrorism efforts.[53]

---

[47] Ibid.

[48] Ibid.

[49] Ibid.

[50] Ibid.

[51] Ibid.

[52] David E. Sanger, "F.B.I. Chief Says Texas Gunman Used Encryption to Text Overseas Terrorist," *The New York Times*, December 9, 2015, accessed March 9, 2016, http://www.nytimes.com/2015/12/10/us/politics/fbi-chief-says-texas-gunman-used-encryption-to-text-overseas-terrorist.html?_r=0.

[53] Ibid.

In meetings with members of Congress, the White House and the public, FBI Director Comey began to beat the drum louder regarding the dangers of the new reality they were facing.[54] Social media's ubiquity and omnipotence did not have regard for any type of traditional geopolitical borders or boundaries.[55] Social media could radicalize people within the United States, the UK or anywhere else in the West and could connect people directly with an operative like Hussain, and then move to an encrypted app where they could be vetted and given operational orders and training to carry out attacks all under the nose of law enforcement who would have no idea that any such discussions were taking place or what was being said.[56]

On August 2, 2015, the UK-based newspaper *The Sunday Times* published an article claiming Hussain ranked third on the US military's "kill list" of terrorists because of his role in inspiring a wave of "lone wolf" attacks on America and the West from Syria.[57] Only Mohammed Emwazi, the ISIL hostage killer known as "Jihadi John," and Abu Bakr al-Baghdadi, ISIL's leader, are seen as higher-priority targets.[58] On August 13,

---

[54] James Comey, "Statement Before the Senate Select Committee on Intelligence," *Federal Bureau of Investigation*, July 8, 2015, accessed March 9, 2016, https://www.fbi.gov/news/testimony/counterterrorism-counterintelligence-and-the-challenges-of-going-dark.

[55] Ibid.

[56] David E. Sanger, "F.B.I. Chief Says Texas Gunman Used Encryption to Text Overseas Terrorist," *The New York Times*, December 9, 2015, accessed March 9, 2016, http://www.nytimes.com/2015/12/10/us/politics/fbi-chief-says-texas-gunman-used-encryption-to-text-overseas-terrorist.html?_r=0.

[57] Dipesh Gadher, "British Hacker is No 3 on Pentagon 'Kill List'," *The Sunday Times*, August 2, 2015, accessed March 8, 2016, http://www.thesundaytimes.co.uk/sto/news/uk_news/article1588418.ece.

[58] Ibid.

2015 USCENTCOM launched a drone attack against Hussain after receiving information that he was in the vicinity of Raqqa, Syria.[59] Hussain managed to escape, although three civilians were killed and five were wounded in the strike. Hussain was later killed in Raqqa by another drone strike on August 24, 2015. USCENTCOM posted a message on their official media page acknowledging the death of Hussain.[60] According to a statement by US Air Force Colonel Patrick Ryder, not only was Hussain involved in recruiting ISIL sympathizers in the West to carry out lone-wolf style attacks, he was also responsible for releasing the personally identifiable information (PII) of about 1,300 US military and government employees, and specifically sought to direct violence against these groups of Americans.[61]

An article written two months after his death called into doubt Hussain's skills and ability as an actual hacker, but stated his true legacy may rest with his ability to spread ISIL's message and the adoption of new technology and security measures.[62] The article referenced several sources who stated that Hussain was nothing more than a "script kiddie," a derogatory term used in the developer community to connote someone

---

[59] Terri Moon Cronk, "Iraq Progresses in ISIL Fight, Key Extremist Confirmed Dead," *U.S. Department of Defense*, August 28, 2015, accessed March 8, 2016, http://www.defense.gov/News-Article-View/Article/615305.

[60] Ibid.

[61] Ibid.

[62] Meg King, "Opinion: The Shocking Mediocrity of Islamic State 'Hacker' Junaid Hussain," *The Christian Science Monitor*, October 26, 2015, accessed March 8, 2016, http://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/1026/Opinion-The-shocking-mediocrity-of-Islamic-State-hacker-Junaid-Hussain.

who possessed negligible skill and merely imitated rather than innovated.[63] According to these sources, the code Hussain used was not his own and was of unsophisticated design.[64] In addition, the article claims that the 1,300 US military names that Hussain reportedly "hacked," was in fact a tasking outsourced to a hacker in Eastern Europe who did the hack for a contracted fee, thus calling into question Hussain's personal technical prowess.[65] However, as the article pointed out, Hussain's example was "sobering because he was trivial, not exceptional," and that anyone could learn to do what Hussain could do.[66] The lesson, then, to be taken from the life, work, and death of Junaid Hussain is that he was a mediocre hacker, and that he was a threat because, as a mediocre hacker, he offered the Islamic State an effective role model.[67] The article concluded that Hussain's example will outlive him, as "[d]rone strikes don't stamp out inspiration."[68]

[63] Ibid.

[64] Ibid.

[65] Ibid.

[66] Ibid.

[67] Ibid.

[68] Ibid.

CHAPTER 4

PRIVACY

While Hussain and other terrorists' use of secure communications are at the center of the government's debate for access to secure communications platforms and encrypted data, Edward Snowden and the classified information he released concerning NSA's extensive surveillance activities are at the center of the privacy debate favoring end-to-end encryption and perfect forward secrecy. Lauded by many as the catalyst for the recognition that privacy was under attack from government action worldwide, Edward Snowden helped usher in the current environment of secure communications and the popularity of encryption. This chapter will focus on the privacy debate, from Edward Snowden to the Arab Spring and back to the debate on terrorism and potential issues arising from Snowden's actions.

Snowden was employed by the firm Booz Allen Hamilton as an IT contractor for the NSA.[1] He was stationed at several locations, including Geneva, Switzerland, where he first became concerned with some of the NSA's intelligence practices in 2008.[2] At that time, he considered disclosing information about the agency's surveillance practices, but decided against it after the election of Barack Obama, whom he hoped would put limits

[1] Janet Reitman, "Snowden and Greenwald: The Men Who Leaked the Secrets," *Rolling Stone*, December 4, 2013, accessed March 11, 2016, http://www.rollingstone.com/politics/news/snowden-and-greenwald-the-men-who-leaked-the-secrets-20131204.

[2] Ibid.

on the NSA and some of its domestic surveillance programs.[3] Seeing no change in the policies of the new administration and Congress, Snowden decided to take matters into his own hands.[4] In 2011, while assigned at an NSA facility in Hawaii, Snowden copied highly classified files from the NSA onto a memory stick and fled to Hong Kong, China, under the false pretense of seeking treatment for his epilepsy.[5] Citing a breach of public trust, Snowden passed the files to three reporters.[6] While in Hong Kong, the first article about the NSA's surveillance programs was published.[7] Snowden singled himself out as the leaker of the classified material, supposedly to protect the journalists who were assisting him.[8] The US government immediately revoked his passport and sought his extradition back to the United States.[9] However, even with his passport revoked, Snowden managed to leave Hong Kong and make his way to Moscow, where he currently resides.[10]

The leaked documents at the center of public criticism centered around the NSA's bulk cell phone data exploitation, perhaps due in part to the ubiquitous and pervasive

---

[3] Ibid.

[4] Ibid.

[5] Ibid.

[6] Ibid.

[7] Ibid.

[8] Ibid.

[9] Bryan Burrough, "The Snowden Saga: A Shadowland of Secrets and Light," *Vanity Fair*, May 2014, accessed March 11, 2016, http://www.vanityfair.com/news/politics/2014/05/edward-snowden-politics-interview.

[10] Ibid.

nature of mobile devices in the everyday lives of almost every American. *The New York Times* had released an NSA slide presentation titled, "Converged Analysis of Smartphone Devices: Identification/Processing/Tasking – All in a day's work."[11] The slide presentation, created in 2010, discussed the history of the smartphone and its ability to change the way the NSA can target and extract information.[12] One slide in particular highlighted the value of a smartphone for data collection purposes by using a scenario involving a photo taken using a smartphone. Should that data be intercepted, the Agency could get the individual's geo-location, the mobile network service provider, website history, type of encryption used, "buddy lists" and networks.[13] This disclosure prompted many technology companies to reevaluate on how they ensured privacy protection. Apple eventually implemented end-to-end encryption on its mobile operating system, iOS 8 in order to prevent the sort of hacking described in the NSA leaks.[14] As a result of this decision, Apple does not have access to the encryption keys, and if presented a legal court order, such as a search warrant to obtain user data, Apple has no way to bypass the encryption to determine what the data reveals. [15]

---

[11] "From the National Security Agency," *The New York Times*, January 27, 2014, accessed March 9, 2016, http://www.nytimes.com/interactive/2014/01/28/world/28mobile-annotateA.html?_r=0.

[12] Ibid.

[13] Ibid.

[14] Roger Fingas, "Edward Snowden Hails Apple as 'Pioneering' for iOS 8 Security Measures," *Apple Insider*, June 5, 2015, accessed March 11, 2016, http://appleinsider.com/articles/15/06/05/edward-snowden-hails-apple-as-pioneering-for-ios-8-security-measures.

[15] Ibid.

Despite some of the dangerous effects of encryption on national security as described earlier, many privacy advocates maintain the importance and benefits of encryption and secure messaging. Instead of thinking in terms of "privacy," Wickr CEO Nico Sell prefers the term "ownership" or "control." According to Sell, "[t]hat issue of control for me is why I've always boycotted Facebook. Because I didn't want to give my network, my friends, my pictures to someone else to own and control for the rest of history."[16] Sell created Wickr in 2011, roughly two years prior to the Snowden leaks.[17] At the time, Sell wanted to create an app that could guard against the theft or collection of user data by technology companies such as Google, Facebook, Yahoo and Microsoft, which generated billions of dollars in revenue generated through user data collected from their customers.[18] Wickr allows users to auto delete their messages and data on the app through their 'shredder' feature.[19] This is a key difference from traditional platforms where "most technical systems are architected in ways that prioritize keeping data," notes Danah Boyd, a Senior Researcher at Microsoft Research.[20] Previously, storing data was

[16] Will Bourne, "Birth of the Resistance," *Inc* 36, no. 6 (July 2014): 24-30, *Academic Search Premier,* EBSCO*host*, accessed February 22, 2016.

[17] Ibid.

[18] Ibid.

[19] Kit Eaton, "These Apps Promise to Encrypt Your Smartphone Communications," *The New York Times,* March 24, 2016, March 25, 2016, http://www.nytimes.com/2016/03/24/technology/personaltech/encryption-by-app-adds-security-to-smartphones.html?_r=0.

[20] Esther Shein, "Ephemeral Data," *Communications Of The ACM* 56, no. 9 (September 2013): 20-22, *Academic Search Premier*, EBSCO*host*, accessed March 8, 2016.

cost prohibitive and as a consequence, much data was "thrown away" or deleted due to lack of available server space.[21]

The creation of secure messaging apps allowed users to better control the information they share, and to block out both business and government interests.[22] These new social media and communications apps charted the way forward for "ephemeral data."[23] The term was popularized after the development of social media apps such as Snapchat, Gryphn and Wickr.[24] These apps were revolutionary because users' data, in the form of a chat message or a photo sent to another user, would have a set timer on when the message would 'self-destruct' or delete permanently.[25] This function made users feel that they could be more open in their discussions without fear of having their private conversations spied upon or having their data freely available for marketers. According to Silent Circle's Chief Technology Officer (CTO) Jon Callas, "Ephemeral data isn't new — what's new is we have enough compute power and enough storage to record everything. That's relatively new in human history…It's simultaneously intriguing and creepy."[26]

---

[21] Ibid.

[22] Hilton Collins, "3 Technologies Claiming to Secure Messages in the Post-Snowden Era," *Government Technology*, July 10, 2014, accessed March 5, 2016, http://www.govtech.com/videos/3-Techs-Claim-to-Secure-Messages-in-the-Post-Snowden-Era.html.

[23] Esther Shein, "Ephemeral Data," *Communications Of The ACM* 56, no. 9 (September 2013): 20-22, *Academic Search Premier*, EBSCO*host*, accessed March 8, 2016.

[24] Ibid.

[25] Ibid.

[26] Ibid.

Secure messaging apps are changing the way users, including terrorists, share information.[27] Telegram, founded by Russian national Pavel Durov, who is also responsible for the Russian answer to Facebook, VKontakte, gained notoriety as the messaging app of choice for ISIL and ISIL supporters and operatives.[28] This is due in part to a function that allows the creation of secure "channels" that allow users to securely broadcast information or news to thousands of other users.[29] This function has allowed ISIL to broadcast their propaganda and connect with sympathizers around the globe without worry that their information flow will be disrupted by Spy Agencies.[30] For example, one channel, the Amaq News Agency utilizes Telegram to put out the latest news on the Islamic State.[31] "It has become much more assimilated into the Islamic State's propaganda infrastructure, and now it's a fully fledged and very important part of it. It has become the first point of publication for claims of responsibility by the group — though not as a rule", stated Charlie Winter, a senior researcher at the Transcultural Conflict and Violence Initiative at Georgia State University.[32] Another channel,

---

[27] Rukmini Callimachi, "A News Agency With Scoops Directly From ISIS," *New York Times,* January 15, 2016., A10, *Academic Search Premier,* EBSCO*host,* accessed February 27, 2016.

[28] Doug Bolton, "Telegram Founder Knew ISIS was Using the App to Communicate Before Paris Attacks," *The Independent*, November 20, 2015, accessed March 5, 2016, http://www.independent.co.uk/life-style/gadgets-and-tech/news/telegram-knew-isis-communicate-paris-pavel-durov-a6742126.html.

[29] Ibid.

[30] Ibid.

[31] Rukmini Callimachi, "A News Agency With Scoops Directly From ISIS," *New York Times,* January 15, 2016., A10, *Academic Search Premier,* EBSCO*host,* accessed February 27, 2016.

[32] Ibid.

"Information Security," encourages Belgian ISIS supporters to use encryption if they access the internet and warns "Intelligence agencies will work all day and night to catch any jihadi in Belgium, so be ready to act,"[33].ISIL's use of Telegram has not dissuaded Durov, who fled Russia after he was forced out of his company for refusing to block certain protest groups from using VKontakte.[34] In addition, Durov stated that one of his main reasons for creating Telegram "was to build a means of communication that can't be accessed by the Russian security agencies."[35] Durov argued in September 2015 at the TechCrunch Disrupt conference in San Francisco, California that "[u]ltimately ISIL will find a way to communicate with its cells, and if any means doesn't feel secure to them, they'll [find something else]. We shouldn't feel guilty about it. We're still doing the right thing protecting our users' privacy."[3637]

[33] Pamela Engel, "A Pro-ISIS Account is Giving its Belgian Followers Specific Instructions on How to Evade Authorities," *Business Insider*, March 22, 2016, accessed March 23, 2016, http://www.businessinsider.com/isis-belgian-supporters-encryption-2016-3.

[34] Christopher Miller, "A Long Way From Moscow," *Mashable*, May 18, 2015, accessed March 5, 2016, http://mashable.com/2015/05/18/russias-mark-zuckerberg-pavel-durov/#zr1.klvXSkq9.

[35] James Vincent, "Telegram Messenger: App Built to Foil Russian Spies Soars After WhatsApp Trouble," *The Independent*, February 26, 2014, accessed March 5, 2016, http://www.independent.co.uk/life-style/gadgets-and-tech/telegram-messenger-app-built-to-foil-russian-spies-soars-after-whatsapp-trouble-9154720.html.

[36] Paz Shabtai, "Paris Attacks Raise Privacy Debate Once More," *iHLS*, November, 20, 2015, accessed March 5, 2016, http://i-hls.com/2015/11/paris-attacks-raise-privacy-debate-once-more/.

[37] Sarah Kaplan "Founder of App Used By ISIS Once Said 'We Shouldn't Feel Guilty'. On Wednesday He Banned Their Accounts," *The Washigton Post*, November 19, 2015, accessed March 9, 2016. https://www.washingtonpost.com/news/morning-mix/wp/2015/11/19/founder-of-app-used-by-isis-once-said-we-shouldnt-feel-guilty-on-wednesday-he-banned-their-accounts/.

ISIS may indeed be looking to find something else. In January 2016, *The Atlantic* published an article titled, "The Flaw in ISIS's Favorite Messaging App."[38] The article discussed a recent auditing of Telegram's source code by associate professor Claudio Orlandi and his graduate researcher Jakob Jakobsen at Denmark's Aarhaus University.[39] Telegram, unlike many other secure messaging apps, does not utilize open source cryptography protocols, instead favoring a custom protocol, MTProto, that Telegram designed in-house.[40] Some cryptographers have expressed puzzlement at this decision by Telegram, as the open source code cryptography has been vetted and improved over many iterations. As the article states, "The more novel an approach to encryption is, the less time researchers have had to spot vulnerabilities…. [T]he more unusual or non-standard an encryption scheme is, the more difficult it can be to identify points of failure that are hidden in a tangle of unconventional choices."[41] Orlandi and his assistant were able to spot a potential flaw in Telegram's protocol—the lack of a property called "indistinguishability under chosen ciphertext attack" of IND-CCA.[42] While the flaw was considered very minor and more a "theoretical" flaw, it was noteworthy in the fact that

[38] Clary Grayson, "The Flaw in ISIS's Favorite Messaging App," *The Atlantic*, January 4, 2016, accessed March 11, 2016, http://www.theatlantic.com/technology/archive/2016/01/isiss-favorite-messaging-app-has-a-security-problem/422460/.

[39] Ibid.

[40] Ibid.

[41] Ibid.

[42] Ibid.

the odds of the custom protocol having only one flaw are quite small. [43] In addition to concerns about the security of its custom encryption protocol, Telegram service began to take action against ISIL's use of Telegram channels by deleting extremist channels from them from the app.[44] These actions have prompted ISIL to consider creating its own custom security application.[45] However, much like with Telegram's MTProto custom protocol, security analysts and cryptographers believe that it would be a risky venture for ISIL to create something new when the open source protocols have withstood the test of time.[46] Perhaps shaking the Islamic State's confidence on the invulnerability of certain secure messaging may play into the hands of those targeting the group and provide a way to exploit their fears.

In March 2016, twin bomb attacks occurred in the Belgian capital of Brussels, targeting the Brussels airport and the subway station.[47] The attacks claimed 32 lives and left over 300 wounded.[48] In the wake of the attacks, the discussion again has focused on how the terrorists were able to plan the operations under such heightened security.[49]

---

[43] Ibid.

[44] Ibid.

[45] Ibid.

[46] Ibid.

[47] Valentina Pop, "Belgium Warns of Terror Risk as Second Brussels Bombing Suspect Is Charged in Paris Attack," *The Wall Street Journal*, April 19, 2016, accessed April 19, 2016, http://www.wsj.com/articles/belgium-still-at-risk-of-terror-attack-1461069025.

[48] Ibid.

[49] Pamela Engel, "A Pro-ISIS Account is Giving its Belgian Followers Specific Instructions on How to Evade Authorities," *Business Insider*, March 22, 2016, accessed March 23, 2016, http://www.businessinsider.com/isis-belgian-supporters-encryption-2016-3.

In an interview with CBS Evening News's Scott Pelley, NYPD deputy commissioner of intelligence and counterterrorism, John Miller stated:

> I think the real point here is we're looking at we call 'going dark,' whether it's the app Telegram …which was all encrypted, or the app Wickr, which comes out of San Francisco, not Russia, that is all encrypted…We're seeing not just iPhones that can't be cracked, but entire communication systems that are designed to be impenetrable, and we're seeing those become the primary tools of terrorists. So when you ask a question like 'How could they miss this?' technology is becoming a big enabler.[50]

However, to advocates, strong protection is necessary in order to help guarantee the privacy and safety of individuals from potentially oppressive regimes that have greater resources and power than the average citizen. The Arab Spring revolts that took place across North Africa and the Arabian Peninsula in 2011 underscored the critical need for having programs that could help users stay secure and remain anonymous while broadcasting their message to the public.[51] This was evident in Egypt, where the masses were empowered to challenge oppressive regime of Hosni Mubarak that had ruled Egypt for three decades.[52] The uprising in Egypt was dubbed the "Twitter Revolution" as the Egyptian people began to use the microblogging service to send quick messages about

[50] "Top NYPD Official: 'Technology Is Becoming A Big Enabler' In Terrorists Secretly Planning Attacks," *CBS New York*, March 22, 2016, accessed March 23, 2016, http://newyork.cbslocal.com/2016/03/22/john-miller-nypd-brussels-attacks/.

[51] Cyrus Farivar, "From Encryption to Darknets: As Governments Snoop, Activists Fight Back," *Ars Technica,* February 15, 2012, accessed March 4, 2016, http://arstechnica.com/business/2012/02/from-encryption-to-darknets-as-governments-snoop-activists-fight-back/.

[52] Sam Gustin, "Social Media Sparked, Accelerated Egypt's Revolutionary Fire," *Wired*, February 11, 2011, accessed March 5, 2016, http://www.wired.com/2011/02/egypts-revolutionary-fire/.

what was happening and as a call to join the protests in Tahrir Square.[5354] As messages were being spread more quickly and forwarded to broader audiences via Twitter, more and more people were moved to join the protests in Tahrir Square.[55] Sascha Meinrath, director of the New America Foundation's Open Technology Initiative stated that "In the same way that pamphlets didn't cause the American Revolution, social media didn't cause the Egyptian revolution…Social media have become the pamphlets of the 21st century, a way that people who are frustrated with the status quo can organize themselves and coordinate protest, and in the case of Egypt, revolution."[56] Currently in Egypt, Twitter and social media in general are considered the best means to protect themselves from the government.[57] As one Egyptian commented to The Daily Beast, social media "is the only thing that scares them [Egyptian government]"[58]

While many privacy activists laud Edward Snowden for risking everything in order to expose what he considered a moral stain against the United States, there are

---

[53] Nancy Youssef, "Egypt's Second Twitter Revolution," *The Daily Beast*, December, 10, 2015, accessed March 5, 2016, http://www.thedailybeast.com/articles/2015/12/11/egypt-s-second-twitter-revolution.html.

[54] Dan Murphy, "Inspired By Tunisia, Egypt's Protests Appear Unprecedented," *The Christian Science Monitor*, January 25, 2011, accessed March 5, 2016, http://www.csmonitor.com/World/Backchannels/2011/0125/Inspired-by-Tunisia-Egypt-s-protests-appear-unprecedented.

[55] Ibid.

[56] Ibid.

[57] Sam Gustin, "Social Media Sparked, Accelerated Egypt's Revolutionary Fire," *Wired*, February 11, 2011, accessed March 5, 2016, http://www.wired.com/2011/02/egypts-revolutionary-fire/.

[58] Nancy Youssef, "Egypt's Second Twitter Revolution," *The Daily Beast*, December, 10, 2015, accessed March 5, 2016, http://www.thedailybeast.com/articles/2015/12/11/egypt-s-second-twitter-revolution.html.

others who argue that Edward Snowden has weakened the United States and its ability to conduct legitimate foreign intelligence gathering.[59] Nation-states and terrorists groups such as the Islamic State have learned how the Government collects information from the leaked NSA materials.[60] In a February 12, 2015 hearing to the Senate Select Committee on Intelligence, National Counterterrorism Center (NCTC) Director Nicholas Rasmussen told the committee:

> Due to the Snowden leaks and other disclosures, terrorists also have a great understanding of how we seek to conduct surveillance, including our methods, our tactics and the scope and scale of our efforts. They've altered the ways in which they communicate and this has led to a decrease in collection…We have specific examples…of terrorists who have adopted greater security measures such as using various new types of encryption, terrorists who have dropped or changed email addresses, and terrorists who have simply stopped communicating in ways they had before, in part because they understand how we collected.[61]

In an interview with CNN's Jim Sciutto in October 2014, former NCTC Director Matthew Olsen, expressed the same concern: "We've lost collection against some individuals [and] lost insight into what they were doing....They've changed how they encrypt their communications and adopted more stringent encryption techniques,

---

[59] Steven Aftergood, "Leaks Damaged U.S. Intelligence, Official Says," *Federation of American Scientists*, February 17, 2015, accessed March 11, 2016, https://fas.org/blogs/secrecy/2015/02/leaks-damaged/.

[60] Eric Schmitt, "ISIS Leader Takes Steps to Ensure Group's Survival," *The New York Times*, July 21, 2015, February 29, 2016, http://www.nytimes.com/2015/07/21/world/middleeast/isis-strategies-include-lines-of-succession-and-deadly-ring-tones.html?_r=0.

[61] Steven Aftergood, "Leaks Damaged U.S. Intelligence, Official Says," *Federation of American Scientists*, February 17, 2015, accessed March 11, 2016, https://fas.org/blogs/secrecy/2015/02/leaks-damaged/.

chang[ing]service providers and email addresses, and …in some cases, just dropped off all together."[62] Former CIA Deputy Director Michael Morrell wrote in his memoir:

> Within weeks of the leaks, terrorist organizations around the world were already starting to modify their actions in light of what Snowden disclosed. Communications sources dried up, tactics were changed…Terrorist groups including ISIS, have since shifted their communications to more "secure" platforms, are using encryption, or are avoiding electronic communications altogether…ISIS was one of those terrorist groups that learned from Snowden, and its clear that his actions played a role in the rise of ISIS.[63]

In response to Laura Poitras's documentary on Edward Snowden, *Citizenfour,* Michael Cohen of *The Daily Beast* remarked "What is left out of Poitras's highly sympathetic portrayal of Snowden is so much of what we still don't know about him. For example, why did he steal so many documents that have nothing to do with domestic surveillance but rather overseas–and legal–intelligence-gathering operations?".[64] Fred Kaplan, who also reviewed the film stated "Whatever you think about foreign intelligence operations, the NSA's core mission *is* to intercept communications of foreign governments and agents. If Snowden and company wanted to take down an intelligence agency, they should say so. But that has nothing to do with whistleblowing or

---

[62] Kevin Liptak, "Ex-counterterrorism Chief: U.S. Lost Track of Terrorists After Snowden," *CNN,* October 21, 2014, accessed March 11, 2016, http://www.cnn.com/2014/10/21/politics/olsen-nsa/index.html.

[63] Shane Harris, "CIA's Ex-No. 2 Says ISIS 'Learned From Snowden'," *The Daily Beast*, May 6, 2015, accessed March 11, 2016, http://www.thedailybeast.com/articles/2015/05/06/cia-s-ex-no-2-says-isis-learned-from-snowden.html.

[64] Steven Aftergood, "Leaks Damaged U.S. Intelligence, Official Says," *Federation of American Scientists*, February 17, 2015, accessed March 11, 2016, https://fas.org/blogs/secrecy/2015/02/leaks-damaged/.

constitutional rights."[65] However one chooses to view Edward Snowden there is no doubt that he has single handedly driven the debate on the tradeoffs between privacy and security and the use of encryption. The question is whether the reaction to the surveillance programs has created an environment that has swung too far towards the privacy side and thus put the security of the United States and its allies at risk at home and abroad.

[65] Fred Kaplan, "Sins of Omission," *Slate*, October 16, 2014, accessed March 12, 2016, http://www.slate.com/articles/news_and_politics/war_stories/2014/10/citizenfour_review_laura_poitras_edward_snowden_documentary.html.

CHAPTER 5

LEGISLATION

In an October 2015 session of the Homeland Security and Governmental Affairs Committee, FBI Director James Comey announced that "The administration has decided not to seek a legislative remedy now, but it makes sense to continue conversations with industry."[1] This echoed statements the FBI Director made in July 2015 in an appearance before the Senate Judiciary and House Intelligence Committees where the Director stated "while there has not yet been a decision whether to seek legislation, we must work with Congress, industry academics, privacy groups, and others to craft an approach that addresses all of the multiple, competing legitimate concerns that have been the focus of so much debate in recent months."[2] Similarly, the White House's National Security Council spokesman Mark Stroh commented that "As the president has said, the United States will work to ensure that malicious actors can be held to account – without weakening our commitment to strong encryption. As part of those efforts, we are actively engaged with private companies to ensure they understand the public safety and national security risks that result from malicious actors' use of their encrypted products and

[1] Ellen Nakashima, "Obama Administration Opts Not to Force Firms to Decrypt Data – for Now," *Washington Post*, October 8, 2015, accessed March 12, 2016, https://www.washingtonpost.com/world/national-security/obama-administration-opts-not-to-force-firms-to-decrypt-data--for-now/2015/10/08/1d6a6012-6dca-11e5-aa5b-f78a98956699_story.html.

[2] James Comey, "Joint Statement with Deputy Attorney General Sally Quillian Yates Before the Senate Judiciary Committee," *Federal Bureau of Investigation*, July 8, 2015, accessed March 9, 2016, https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy.

services."[3] With the decision in October the White House signaled that it was walking a tightrope between the needs of the Department of Justice and the demands of technology companies and the American public.[4]

In the month following Director Comey's remarks to the Homeland Security and Governmental Affairs Committee, on November 13, 2015, seven armed terrorists divided into three groups launched a deadly wave of attacks against the citizens of Paris, killing 132 and wounding hundreds more.[5] The terrorists attacked three main targets: 1) the Stade de France, where an international soccer match was taking place between France and Germany, 2) the nightlife district of Paris, bustling with restaurants and bars, and 3) the Bataclan concert hall, where the American rock group *The Eagles of Death Metal* were performing.[6] Attackers detonated explosive vests outside the Stade de France,[7] while another group of attackers targeted various restaurants and bars in the nightlife district of Paris. [8] The largest number of casualties were reported at the Bataclan concert hall, where 89 people were killed when 4 attackers armed with Kalashnikov rifles and

[3] Ellen Nakashima, "Obama Administration Opts Not to Force Firms to Decrypt Data – for Now," *Washington Post*, October 8, 2015, accessed March 12, 2016, https://www.washingtonpost.com/world/national-security/obama-administration-opts-not-to-force-firms-to-decrypt-data--for-now/2015/10/08/1d6a6012-6dca-11e5-aa5b-f78a98956699_story.html.

[4] Ibid.

[5] "Paris Attacks: What Happened on the Night," *BBC News*, December 09, 2015, accessed March 9, 2016, http://www.bbc.com/news/world-europe-34818994.

[6] Ibid.

[7] Ibid.

[8] Ibid.

suicide explosive vests stormed in and began firing on the crowd.[9] The following day, ISIL claimed responsibility for planning and coordinating the Paris attacks from abroad.[10] French President Francoise Hollande declared the attacks an "an act of war committed by Daesh [ISIL] that was prepared, organized and planned from outside [France]"[11]

In the wake of the attacks, US intelligence officials indicated that ISIL probably used secure messaging applications, specifically SnapChat and Telegram, to coordinate the attacks.[12] Privacy rights activists, however, argued against assigning a prominent role to encrypted apps, pointing to a 55-page report by the French anti-terrorism police that emphasized the fact that the attackers used so-called "burner phones" --cheap, disposable phones-- that were only activated days or even hours before the attack.[13,14] Details about the planning and coordination of the attacks are still emerging, and government authorities hope to obtain more intelligence now that the only perpetrator to survive the

[9] Ibid.

[10] "Hollande Calls Paris Attacks An 'Act of War'," *Al Jazeera*, November 14, 2015, accessed March 10, 2016, http://www.aljazeera.com/news/2015/11/hollande-paris-france-attacks-concern-stadium-isil-151114103631610.html.

[11] Ibid.

[12] Evan Perez, "First on CNN: Paris Attackers Likely Used Encrypted Apps, Officials Say," *CNN*, December 17, 2015, accessed March 13, 2016, http://www.cnn.com/2015/12/17/politics/paris-attacks-terrorists-encryption/.

[13] Rukmini Callimachi, "A View of ISIS's Evolution in New Details of Paris Attack," *The New York Times*, March 19, 2016, accessed March 25, 2016, http://www.nytimes.com/2016/03/20/world/europe/a-view-of-isiss-evolution-in-new-details-of-paris-attacks.html?_r=0.

[14] Glyn Moody, "Paris Terrorists Used Burner Phones, Not Encryption, To Evade Detection," *Ars Technica*, March 21, 2016, accessed March 26, 2016, http://arstechnica.com/tech-policy/2016/03/paris-terrorist-attacks-burner-phones-not-encryption/.

attacks, Salah Abdesalam, was apprehended on March 18, 2016 in a police raid by Belgium authorities.[15]

A few weeks after the Paris attacks, on December 2, 2015, two ISIL supporters in the United States—Syed Rizwan Farook and his wife, Tashfeen Malik--coordinated a mass shooting and attempted bombing attack at a holiday party at the Inland Regional Center in San Bernadino, California.[16] Shortly after killing 14 people and wounding 22 others in the deadliest terrorist attack in the United States since 9/11,[17] Farook and Malik publicly pledged allegiance to ISIL's leader, Abu Bakr Al-Baghdadi, via social media.[18] Malik's message concluded with the hope that their attack would 'awaken' Muslims across the United States, Europe and Australia.[19]

ISIL's official English language magazine, *Dabiq,* was quick to praise the attackers saying, "How much more deserving of Allah's blessing are a husband and wife who march out together to fight crusaders in defense of the Khilifah…terroriz[ing] [the]

---

[15] "Paris Attacks: What Happened on the Night," *BBC News*, December 9, 2015, accessed March 9, 2016, http://www.bbc.com/news/world-europe-34818994.

[16] Calamur, Krishnadev, Marina Koren, and Matt Ford, "A Day After the San Bernadino Shooting," *The Atlantic*, December 3, 2015, accessed March 16, 2016, http://www.theatlantic.com/national/archive/2015/12/a-shooter-in-san- bernardino/418497/.

[17] Richard Winton, "Why Brussels Attacks Exceeded San Bernadino's: A Terrorist Infrastructure," *Los Angeles Times*, March 22, 2016, accessed March 25, 2016, http://www.latimes.com/local/lanow/la-me-ln-terrorist-infrastructure-brussels-vs-san-bernardino-20160322-story.html.

[18] Richard Winton, "San Bernadino Shooters Praised by Islamic State Magazine," *Los Angeles Times*, January 20, 2016, accessed March 15, 2016, http://www.latimes.com/local/lanow/la-me-ln-islamic-state-magazine-san-bernardino-terrorists-20160120-story.html.

[19] Ibid.

crusaders in their very strongholds."[20] The investigation into the attacks is ongoing and officials have yet to disclose whether encrypted apps played a role in the attacks. However, the FBI sought to examine the contents of Farook's smartphone, an Apple iPhone 5c.[21] Because encryption was enabled on the smartphone, the FBI was unable to unlock the phone or retrieve its contents from Apple.[22] The FBI sought a court order to compel the company to assist with unlocking the phone, but Apple responded that it would not be able to do anything, due, in part, to the company's encryption scheme.[23] In Apple's brief to US Magistrate Judge James Orenstein, who was considering the Justice Department's request, the company stated:

> In most cases now and in the future, the government's requested order would be substantially burdensome, as it would be impossible to perform. For devices running iOS 8 or higher, Apple would not have the technical ability to do what the government requests—take possession of a password protected device from the government and extract unencrypted user data from that device for the government. Among the security features in iOS 8 is a feature that prevents anyone without the device's passcode from accessing the device's encrypted data. This includes Apple.[24]

The court was scheduled to issue a decision on March 18, 2016, but the decision was postponed after the Department of Justice received information from a third party on

---

[20] Ibid.

[21] Edvard Pettersson, "U.S. Drops Apple Case After Getting Into Terrorist's iPhone," *Bloomberg*, March 28, 2016, accessed April 1, 2016, http://www.bloomberg.com/news/articles/2016-03-28/u-s-drops-apple-case-after-successfully-accessing-iphone-data-imcj88xu.

[22] Ibid.

[23] Joe Palazzolo, "Apple Tells Court It Can't Unlock New iPhones," *The Wall Street Journal*, October 20, 2015, accessed March 20, 2016, http://blogs.wsj.com/law/2015/10/20/apple-tells-court-it-cant-unlock-new-phones/.

[24] Ibid.

how the FBI could bypass Apple's encryption to unlock the iPhone.[25] The case was ultimately dismissed a few days later when the FBI confirmed it was able to unlock the device without the assistance of Apple.[26] It has yet to be determined whether the FBI discovered anything of value on the smartphone, such as information revealing how the attack was planned and if anyone else was involved.[27] The dismissal of the case served to postpone a decision on an issue that will likely reappear before the courts—the ability of the federal government to compel a technology company to compromise or weaken its own technology in order to comply with a government request. In response to this new information revealing an obvious vulnerability in Apple's security measures, privacy advocates have called on the federal government and the FBI to release information on how they were able to bypass Apple's security, arguing that this would enable the company to patch a flaw that may now be exploited by nefarious actors against iPhone users.[28]

With the legal discussion postponed, Congress is considering legislation aimed at creating a commission to explore ways in which privacy and security can be achieved in

[25] Edvard Pettersson, "U.S. Drops Apple Case After Getting Into Terrorist's iPhone," *Bloomberg*, March 28, 2016, accessed April 1, 2016, http://www.bloomberg.com/news/articles/2016-03-28/u-s-drops-apple-case-after-successfully-accessing-iphone-data-imcj88xu.

[26] Ibid.

[27] Ibid.

[28] Sara Sorcher, "Influencers: FBI Should Disclose San Bernadino iPhone Security Hole to Apple," *The Christian Science Monitor*, March 24, 2016, accessed March 26, 2016, http://www.csmonitor.com/World/Passcode/Passcode-Influencers/2016/0324/Influencers-FBI-should-disclose-San-Bernardino-iPhone-security-hole-to-Apple.

tandem.[29] The House Homeland Security Committee introduced legislation creating the National Commission on Security and Technology Challenges, also referred to as the McCaul-Warner Commission on Digital Security. This bi-partisan bill, sponsored by Committee Chairman Michael McCaul (R-TX) and Senator Mark Warner (D-VA), was announced on December 28, 2015, and was designed "to collectively address the larger issue of protecting national security and digital security, without letting encrypted communications become a safe haven for terrorists."[30] The Commission would be composed of experts and practitioners from the technology sector, cryptography, law enforcement, intelligence, the privacy and civil liberties community, global commerce and economics, and the national security community.[31] The Commission would be charged with examining privacy and security issues in a systematic, holistic way, and considering their implications for national security, public safety, data security, privacy, innovation, and American competitiveness in the global marketplace.[32] In order to execute its mission, the Commission would possess the power to issue subpoenas, hold public hearings and

[29] "McCaul, Warner Lead Bipartisan Coalition to Establish National Commission on Digital Security," *House Committee on Homeland Security*, February 29, 2016, accessed on March 17, 2016, https://homeland.house.gov/press/mccaul-warner-lead-bipartisan-coalition-to-establish-national-commission-on-digital-security/.

[30] Ibid.

[31] Michael McCaul, "How to Unite Privacy and Security – Before the Next Terrorist Attack," *The Washington Post*, December 27, 2015, accessed March 17, 2016, https://www.washingtonpost.com/opinions/how-to-unite-privacy-and-security--before-the-next-terrorist-attack/2015/12/27/628537c4-a9b3-11e5-9b92-dea7cd4b1a4d_story.html.

[32] Congress, House, *To Establish in the Legislative Branch the National Commission on Security and Technology Challenges*, 114th Cong., 2d sess., H.R. 4651, https://homeland.house.gov/wp-content/uploads/2016/03/2016.03.03_HR-4651-Commission.pdf.

request any information from executive branch agencies in order to execute their mission.[33] The Commission's activities would culminate in the creation of a report to Congress providing the following: (A) An assessment of the issue of multiple security interests in the digital world, including public safety, privacy, national security, and communications and data protection, both now and throughout the next 10 years.[34]

> (B) A qualitative and quantitative assessment of—
>
> > (i) the economic and commercial value of cryptography and digital security and communications technology to the economy of the United States;
> > (ii) the benefits of cryptography and digital security and communications technology to national security and crime prevention;
> > (iii) the role of cryptography and digital security and communications technology in protecting the privacy and civil liberties of the people of the United States;
> > (iv) the effects of the use of cryptography and other digital security and communications technology on Federal, State, and local criminal investigations and counterterrorism enterprises;
> > (v) the costs of weakening cryptography and digital security and communications technology standards; and
> > (vi) international laws, standards, and practices regarding legal access to communications and data protected by cryptography and digital security and communications technology, and the potential effect the development of disparate, and potentially conflicting, laws, standards, and practices might have.
>
> (C) Recommendations for policy and practice, including, if the Commission determines appropriate, recommendations for legislative changes, regarding—
>
> > (i) methods to be used to allow the United States Government and civil society to take advantage of the benefits of digital security and

[33] Ibid.

[34] Ibid.

> communications technology while at the same time ensuring that the danger posed by the abuse of digital security and communications technology by terrorists and criminals is sufficiently mitigated;
> (ii) the tools, training, and resources that could be used by law enforcement and national security agencies to adapt to the new realities of the digital landscape; (iii) approaches to cooperation between the Government and the private sector to make it difficult for terrorists to use digital security and communications technology to mobilize, facilitate, and operationalize attacks;
> (iv) any revisions to the law applicable to wiretaps and warrants for digital data content necessary to better correspond with present and future innovations in communications and data security, while preserving privacy and market competitiveness;
> (v) proposed changes to the procedures for obtaining and executing warrants to make such procedures more efficient and cost-effective for the Government, technology companies, and telecommunications and broadband service providers; and
> (vi) any steps the United States could take to lead the development of international standards for requesting and obtaining digital evidence for criminal investigations and prosecutions from a foreign, sovereign State, including reforming the mutual legal assistance treaty process, while protecting civil liberties and due process.

It is yet to be seen what the Commission will be able to achieve in the advancement of meaningful legislation on encryption and secure messaging. Hopefully, the Committee can define the problem and begin the discussions between the private sector and the public sector in order to chart a path going forward on meaningful privacy reforms that strike the appropriate balance with regards to security. However, weakening or limiting encryption is a solution that should be avoided at all costs. The potential damage to national security, public trust and American economic competitiveness overseas is too great to justify such a measure. Any potential backdoor or weakness built into an encryption algorithm will provide an avenue for other nation state intelligence organizations, criminal organizations, hackers and terrorists to take advantage for their

benefit. Google provided a backdoor for the US Government under the CALEA program that was breached by the Chinese government in 2009.[35] Again the Chinese government was able to steal the security clearance data of tens of thousands of public sector employees in the United States. That information would be unusable to the Chinese had the information been secured through encryption.[36] There have been numerous cases of massive data breaches of consumer information that have been stolen from companies such as Target, Sony Pictures, JPMorgan and BlueCross Blue Shield—all of which could have been avoided with improved encryption.[37]

The exposure of government mandates into American consumer technology products has eroded trust overseas and has made American technology less desirable. This has the potential to be the biggest impact from the Snowden fallout as it hurts American competitiveness overseas. As mentioned in Chapter 1, some estimates at the economic impact from these revelations and the government prior work with American companies are as high as $180 billion. The U.S.-E.U. Data Protection safe harbor, which provided a legal framework since the turn of the century for commercial cross-border data flows, was recently ruled invalid by the Court of Justice of the European Union due

[35] "Don't Panic: Making Progress on the "Going Dark Debate," *Berkman Center for Internet & Society*, February 1, 2016, accessed March 17, 2016, https://cyber.law.harvard.edu/publications/2016/Cybersecurity/Dont_Panic.

[36] Ibid.

[37] Kevin Granville, "9 Recent Cyberattacks Against Big Business," *The New York Times*, February 5, 2015, accessed March 9, 2016, http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html?_r=0.

to concern that the U.S. intelligence community may be able to gain access to that data.[38] Also mentioned earlier, the Brazilian government is looking to make a shift away from the use of American technology products due to the perception that American intelligence has was to access the data that resides within the products. Such views will hurt the American economy and prestige overseas. Steps that companies such as Apple and Google are doing in providing full end-to-end encryption are ways to counter the negative press they received as a result of the Snowden revelations. If countries feel that all data is protected in transit through encryption the more likely they will be to regain trust in that technology and continue to place orders for American technology. Solving one problem, that of terrorist use of secure encrypted messaging to communicate would only create much larger problems. In addition, such a victory against the terrorists would be short-lived as they will just move to other techniques to obfuscate authorities as was revealed in the Paris attacks that in addition to using encryption technology the attackers used a much older, cruder solution in purchasing many low cost throw-away or 'burner' phones and multiple SIM cards to evade detection. Terrorists will continue to evolve and will work around attempts to stifle encryption. However, it will be a magnitude harder for the United States to recover economically and repair its reputation at home and aboard just to provide a temporary relief against terrorist communications. When weighed against an economic, humanitarian and civil liberties point of view the argument against encryption seems short-sighted. So what can the government do?

---

[38] "Don't Panic: Making Progress on the "Going Dark Debate," *Berkman Center for Internet & Society*, February 1, 2016, accessed March 17, 2016, https://cyber.law.harvard.edu/publications/2016/Cybersecurity/Dont_Panic.

CHAPTER 6

CONCLUSION/RECOMMENDATIONS

In response to the government's claims of "going dark " on terrorist plotting and other significant criminal activities, a recent Harvard study sought to determine whether the government was, in fact, "going dark" with the advent of secure communications.[1] The study concluded that while encryption and secure messaging services made government surveillance more difficult in certain cases, that did not necessarily mean the government was completely "going dark." Rather, the report stated that "the landscape is far more variegated than the metaphor suggests, and while there are and perhaps always will be "pockets of dimness and some dark spots – communications channels resistant to surveillance, some areas are more illuminated now than in the past, and others are brightening."[2]

As discussed earlier, the FBI and the Intelligence Community have focused their efforts on the "going dark" on the threat posed by terrorists. Secure messaging applications such a Telegram are now able to radicalize individuals and provide would-be terrorists with training and direction without necessarily having to communicate with

[1] "Don't Panic: Making Progress on the "Going Dark Debate," *Berkman Center for Internet & Society*, February 1, 2016, accessed March 17, 2016, https://cyber.law.harvard.edu/publications/2016/Cybersecurity/Dont_Panic.

[2] Ibid.

anyone, further helping to evade detection.[3] With that in mind, can technology companies self-police? The recent action by Telegram may provide a possible answer.[4] In December 2015, Telegram took down 78 'Channels' across 12 languages that were used to spread ISIL messaging.[5] In a statement posted on their app, the company explained it was "disturbed to learn that Telegram's public channels were being used by ISIL to spread their propaganda."[6] The company now plans to create a way for users to 'report objectionable material that will then be forwarded for the company to review and potentially remove from the application.[7] This turn comes against Telegram co-founder Pavel Durov's earlier resistance to "banning words" because "terrorists use those to communicate."[8] Telegram's willingness to flag objectionable material is an example of how the government and the public may be able to help put pressure on companies to provide ways to address safety concerns while still maintaining the ability to secure communications.

---

[3] Pamela Engel, "A popular Messaging App Just Dealt a Potential Blow to ISIS," *Business Insider*, November 25, 2015, accessed March 11, 2016, http://www.businessinsider.com/popular-messaging-app-telegram-just-dealt-a-potential-blow-to-isis-2015-11.

[4] Ibid.

[5] Sam Schechner, "Telegram Messenger Blocks 78 Islamic State-Related Channels," *The Wall Street Journal*, November 18, 2015, accessed March 11, 2016, http://www.wsj.com/articles/telegram-messenger-blocks-78-islamic-state-related-channels-1447897021.

[6] Ibid.

[7] Pamela Engel, "A popular Messaging App Just Dealt a Potential Blow to ISIS," *Business Insider*, November 25, 2015, accessed March 11, 2016, http://www.businessinsider.com/popular- messaging-app-telegram-just-dealt-a-potential-blow-to-isis-2015-11.

[8] Ibid.

While there are no guarantees that such a strategy will work, it does provide a potential avenue to explore with regards to a company's terms of service (ToS), the rules a person or organization must observe in order to use a service.[9] If the government and the public can engage in a dialog with the technology companies to ensure that their ToS include the provisions banning the use of hateful and dangerous speech, that could be one way to limit the reach of terrorist organizations and propaganda without hurting the company's commitment to provide secure communications to all users.

Law enforcement and intelligence agencies must learn to adapt to new technology. Encryption is not going away and forcing companies to weaken their own technology or provide special access has the potential to cause grave economic and diplomatic problems for the United States. Rapid technological advances have left new avenues available for law enforcement and other government agencies.[10] Encryption, on its own, is sometimes difficult to implement, and law enforcement agencies may be able to exploit those that have not implemented their security correctly.[11] Even when done correctly, metadata is not encrypted and is able to be exploited.[12] Metadata is structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use,

[9] "Terms of Service," *PC Magazine*, accessed March 28, 2016, http://www.pcmag.com/encyclopedia/term/62682/terms-of-service.

[10] "Don't Panic: Making Progress on the "Going Dark Debate," *Berkman Center for Internet & Society*, February 1, 2016, accessed March 17, 2016, https://cyber.law.harvard.edu/publications/2016/Cybersecurity/Dont_Panic.

[11] Ibid.

[12] Ibid.

or manage an information resource.[13] Metadata is often called data about data or information about information.[14] Metadata can include such information as tagged geocoordinates from a photo taken on a digital camera or phone, cell phone call location, cell phone numbers.[15] With such metadata, law enforcement may not be able to see exactly the conversations taking place between individuals, but they can see that they are talking and could begin to focus on those individuals using the normal tools available to law enforcement.[16] According to the Harvard Study, "[e]ncryption typically does not protect metadata…[d]ata can also be leaked into unencrypted media, through cloud backups and syncing across multiple devices."[17] However, FBI Director James Comey believes that metadata alone is not a solution. He stated "metadata doesn't provide the content of any communication. It's incomplete information, and even this is difficult to access when time is of the essence. I wish we had time in our work, especially when lives are on the line. We usually don't."[18]

---

[13] Ibid.

[14] National Information Standards Organization (NISO) (2004), *Understanding Metadata* (PDF), Bethesda, USA: NISO Press, ISBN 978-1-880124-62-8.

[15] "Don't Panic: Making Progress on the "Going Dark Debate," *Berkman Center for Internet & Society*, February 1, 2016, accessed March 17, 2016, https://cyber.law.harvard.edu/publications/2016/Cybersecurity/Dont_Panic.

[16] Ibid.

[17] "Don't Panic: Making Progress on the "Going Dark Debate," *Berkman Center for Internet & Society*, February 1, 2016, accessed March 17, 2016, https://cyber.law.harvard.edu/publications/2016/Cybersecurity/Dont_Panic.

[18] James Comey, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?," *Federal Bureau of Investigation*, October 16, 2014, accessed March 28, 2016, https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

As mentioned above, cloud computing and storage may also provide a way for law enforcement to legally discover information.[19] " In the simplest terms, cloud computing means storing and accessing data and programs over the Internet instead of your computer's hard drive."[20] Currently, the government is able to obtain information with a search warrant on Apple's cloud backup, iCloud, which is not encrypted like some of Apple's other services.[21] In fact, the FBI was able to obtain data from the San Bernadino shooter's iCloud account.[22] According to Apple, the following outlines everything that iCloud backs up— with every setting turned on, iCloud stores:[23]

- 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

---

[19] "Don't Panic: Making Progress on the "Going Dark Debate," *Berkman Center for Internet & Society*, February 1, 2016, accessed March 17, 2016, https://cyber.law.harvard.edu/publications/2016/Cybersecurity/Dont_Panic.

[20] Dave Gershgorn, "Apple Cares About Your Privacy, Unless You Use iCloud," *Popular Science*, February 19, 2016, accessed March 28, 2016, http://www.popsci.com/apple-cares-about-your-privacy-unless-you-use-icloud.

[21] Ibid.

[22] Ibid.

[23] Ibid.

An article in the New York Times reports that, "Mr. Cook has told colleagues that he still stands by the company's longstanding plans to encrypt everything stored on Apple's myriad devices, services and in the cloud, where the bulk of data is still stored unencrypted,"[24] Until such time, law enforcement and the Intelligence Community should continue to leverage cloud computing, across the technology sector to illuminate areas they may be currently going dark.[25]

For law enforcement and intelligence agencies, adaptation involves looking ahead and being creative to see how new technology or innovations may help uncover new information sources. The Internet of Things (IOT), which is a concept that envisions an interconnected network of machines, sensors and information technology.[26] The Internet of Things Global Standards Initiative defines the Internet of Things as a "global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies."[27] Companies like Nest have created products such as a 'smart thermostat' that can be programmed wirelessly and can collect information

[24] Ibid.

[25] "Don't Panic: Making Progress on the "Going Dark Debate," *Berkman Center for Internet & Society*, February 1, 2016, accessed March 17, 2016, https://cyber.law.harvard.edu/publications/2016/Cybersecurity/Dont_Panic.

[26] Ibid.

[27] "Internet of Things Global Standards Initiative," *International Telecommunication Union*, accessed March 21, 2016, http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx.

through onboard sensors.[28] What kind of information can a thermostat really collect? According to Nest, the following information can be collected:

- Setup information
- Environmental data from the Nest Learning Thermostat's sensors
- Direct adjustments to the device, including temperature or settings
- Heating and cooling usage information
- Technical information from the device[29]

Digging a bit deeper into Nest's privacy statements, setup information consists of the user's address and zip code.[30] It also pulls information from the home's HVAC (Heating, Ventilation and Cooling) systems.[31] The environmental data that can be collected includes movement in a room, temperature, humidity and ambient light.[32] In addition, 2nd generation models of the device also include a microphone that is able to capture information in order to "deliver certain enhanced features," which are not specified.[33] Finally, technical information that can be collected includes Wi-Fi network name (SSID) and password, IP address, email address, mobile location data if connected via smartphone along with Bluetooth data.[34]

---

[28] "Privacy Statement for Nest Products and Services," *Nest Labs*, March 10, 2016, accessed March 22, 2016, https://nest.com/legal/privacy-statement-for-nest-products-and-services/.

[29] Ibid.

[30] Ibid.

[31] Ibid.

[32] Ibid.

[33] Ibid.

[34] Ibid.

One begins to see the possibilities for law enforcement when such a small household device is able to collect such a wealth of information. According to its website, Nest may be able to provide information they collect to a "third party if we believe in good faith that we are required to do so for legal reasons. For example, to respond to legal process, or comply with state and federal laws (or the applicable laws of foreign countries other than the United States)."[35] As much of this technology is relatively new, the potential for privacy abuse is still yet to be seen. However, in 2015, Samsung came under intense criticism after the *Daily Beast* published an article detailing how the company's new 'Smart TVs' collected voice information on users.[36] The Smart TV can connect to the internet, including apps, and it utilizes voice recognition technology to navigate without the need for using a traditional remote control to operate it.[37] However, the article highlighted a disclaimer about the listening function of the device: "Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party."[38] The article quoted Electronic Frontier Foundation (EFF) Intellectual Property Director Corynne McSherry as saying, "If I were the customer, I might like to know who that third party was, and I'd definitely like to know whether my words were being transmitted in a

[35] Ibid.

[36] Shane Harris, "Your Samsung SmartTV Is Spying on You, Basically," *The Daily Beast*, February 5, 2015, accessed March 22, 2016, http://www.thedailybeast.com/articles/2015/02/05/your-samsung-smarttv-is-spying-on-you-basically.html.

[37] Ibid.

[38] Ibid.

secure form." If the transmission is not encrypted, a individual could conceivably turn your TV into an eavesdropping device.[39] A recent survey by TRUSTe, a digital privacy management company, found 35% of Americans owning at least one smart device other than their smartphone with the number one device being a smart TV. About 79% of survey participants said they were concerned about personal information being collected through their smart devices.[40] After much negative press coverage, Samsung clarified that it encrypted the data and that users would be able to disable the voice recognition function.[41]

One of the main ideas for the Internet of Things is that in the future, many of devices in the home will become interconnected and sensors will be able to relay information to other devices in the home automatically.[42] *Wired* magazine, in an article titled "The Internet of Things is Far Bigger Than Anyone Realizes" argues that while that is true, the real value of the Internet of Things is far greater than simple machine to machine information and that cloud computing and storage will be the main driver of the

[39] Ibid.

[40] Samantha Murphy Kelly, "Samsung's TVs Aren't the Only Devices Listening to You," *Mashable*, February 11, 2015, accessed March 27, 2016, http://mashable.com/2015/02/10/smart-devices-listening/#N68IeFmGb5qX.

[41] Shane Harris, "Your Samsung SmartTV Is Spying on You, Basically," *The Daily Beast*, February 5, 2015, accessed March 22, 2016, http://www.thedailybeast.com/articles/2015/02/05/your-samsung-smarttv-is-spying-on-you-basically.html.

[42] Daniel Burrus, "The Internet of Things Is Far Bigger Than Anyone Realizes," *Wired*, November, 2014, accessed March 26, 2016, http://www.wired.com/insights/2014/11/the-internet-of-things-bigger/.

Internet of Things revolution.[43] The author states:

> The Internet of Things really comes together with the connection of sensors and machines. That is to say, the real value that the Internet of Things creates is at the intersection of gathering data and leveraging it. All the information gathered by all the sensors in the world isn't worth very much if there isn't an infrastructure in place to analyze it in real time. Cloud-based applications are the key to using leveraged data. The Internet of Things doesn't function without cloud-based applications to interpret and transmit the data coming from all these sensors. The cloud is what enables the apps to go to work for you anytime, anywhere.[44]

It must be assumed that such convergence will require tremendous amounts of data. What constitutes personal information when so much information becomes interconnected? It has yet to be seen what kind of privacy implications the internet of things will bring.

There must be a balance between the civil liberties of the individual and the security of the state. While encryption and secure messaging will make law enforcement and the Intelligence Community's job more difficult in the short term, it is unlikely encryption and the use of secure messaging apps will provide a permanent safe haven for terrorists and other nefarious actors. Instead, they can be seen as part of the 'growing pains' of a digital revolution happening in this country and around the world.[45] It is difficult to perfectly balance all the competing forces, and there will be many more fights in the future because technology is still undergoing rapid changes. Ultimately, there is no such thing as perfect security or perfect privacy. There are always tradeoffs between the

---

[43] Ibid.

[44] Ibid.

[45] "Don't Panic: Making Progress on the "Going Dark Debate," *Berkman Center for Internet & Society*, February 1, 2016, accessed March 17, 2016, https://cyber.law.harvard.edu/publications/2016/Cybersecurity/Dont_Panic.

two. As one of the Harvard report's authors states, "We're not being asked to choose between security and privacy. We're being asked to choose between less security and more security."[46]

The internet of things has the potential to drastically change the way we interact with personal information. At the heart of the internet of things is the collection of data, much of it personal, that companies will hope to monetize for their benefit. Individuals will at some point also need to evaluate and decide whether there is a saturation point of too much personal information in the hands of the private sector.

This paper focused on the needs of the state versus the individual's right to privacy against the backdrop of several high profile terrorist attacks that have utilized secure communications methods. Even in light of such despicable acts, the government should not pursue legislation or policies that will force undue privacy burden on the American people and American companies. The government can still collect information in legal and viable manners, but that they will need to get ahead of the technology and become more adaptive. The Commission on Digital Security is also a step in the right direction, more for the hope that it will lead to greater dialogue between the government and the private sector. There is great incentive for private sector companies to collect large amounts of data, especially metadata. While it may become more difficult to gain access to certain communications due to encryption, the vast majority collected data held by the private sector is unencrypted and potentially available for the government to

[46] Ibid.

access through proper legal means.[47] In addition, the government and the public can potentially agree on the fact that certain types of violent and extremist speech has no place and they can put pressure through dialogue and popular opinion with companies like Telegram to flag potentially offensive or violent speech.

[47] KeriLynn Engel, "True Private Messaging: 7 Apps to Encrypt Your Chats," *WhoIsHostingThis Blog*, April 29, 2015, accessed March 22, 2016, http://www.whoishostingthis.com/blog/2015/04/29/im-encryption/.

BIBLIOGRAPHY

Abelson, Hal, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, and Bruce Schneier. "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption." *MIT Computer Science and Artificial Intelligence Laboratory*. May 27, 1997. Accessed March 14, 2016. https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/key-study-report.html.

"About EFF." *Electronic Frontier Foundation*. Accessed March 4, 2016. https://www.eff.org/about.

Ackerman, Spencer, Ewen MacAskill and Alice Ross. "Junaid Hussain: British Hacker for ISIS Believed Killed in US Air Strike." *The Guardian*. August 27, 2015. Accessed March 7, 2016. http://www.theguardian.com/world/2015/aug/27/junaid-hussain-british-hacker-for-isis-believed-killed-in-us-airstrike.

Aftergood, Steven. "Leaks Damaged U.S. Intelligence, Official Says." *Federation of American Scientists*. February 17, 2015. Accessed March 11, 2016. https://fas.org/blogs/secrecy/2015/02/leaks-damaged/.

Atkinson, Michelle, and Kenneth Olmstead. "Apps Permissions in the Google Play Store." *Pew Research Center*. November 10, 2015. Accessed March 4, 2016. http://www.pewinternet.org/files/2015/11/PI_2015- 11-10_apps-permissions_FINAL.pdf.

Ball, James, Julian Borger, and Glenn Greenwald. "Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security." *The Guardian*. September 6, 2013. Accessed March 7, 2016. http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

Bolton, Doug. "Telegram Founder Knew ISIS was Using the App to Communicate Before Paris Attacks." *The Independent*. November 20, 2015. Accessed March 5, 2016. http://www.independent.co.uk/life-style/gadgets-and-tech/news/telegram-knew-isis-communicate-paris-pavel-durov-a6742126.html.

Bourne, Will. "Birth of the Resistance." *Inc* 36, no. 6 (July 2014): 24-30. *Academic Search Premier,* EBSCO*host.* Accessed February 22, 2016.

Burr, Richard. "The Debate Over Encryption: Stopping Terrorists From 'Going Dark." *The Wall Street Journal*. December 23, 2015. Accessed March 9, 2016. http://www.wsj.com/articles/stopping-terrorists-from-going-dark-1450914378.

Burrough, Bryan, Sarah Ellison and Suzanna Andrews. “The Snowden Saga: A Shadowland of Secrets and Light.” *Vanity Fair*. May 2014. Accessed March 11, 2016. http://www.vanityfair.com/news/politics/2014/05/edward-snowden-politics-interview.

Burrus, Daniel. “The Internet of Things Is Far Bigger Than Anyone Realizes.” *Wired*. November 2014. Accessed March 26, 2016. http://www.wired.com/insights/2014/11/the-internet-of-things-bigger/.

Calamur, Krishnadev, Marina Koren, and Matt Ford. “A Day After the San Bernadino Shooting.” *The Atlantic*. December 3, 2015. Accessed March 16, 2016. http://www.theatlantic.com/national/archive/2015/12/a-shooter-in-san-bernardino/418497/.

Callimachi, Rukmini. “A News Agency With Scoops Directly From ISIS.” *New York Times,* January 15, 2016., A10, *Academic Search Premier,* EBSCO*host*. Accessed February 27, 2016.

Callimachi, Rukmini, Alissa J. Rubin, and Laure Fourquet. “A View of ISIS’s Evolution in New Details of Paris Attack.” *The New York Times*. March 19, 2016. Accessed March 25, 2016. http://www.nytimes.com/2016/03/20/world/europe/a-view-of-isiss-evolution-in-new-details-of-paris-attacks.html?_r=0.

Cameron, Dell. “Edward Snowden Tells You What Encrypted Messaging Apps You Should Use.” *The Daily Dot*. March 6, 2015. Accessed March 7, 2016. http://www.dailydot.com/politics/edward-snowden-signal-encryption-privacy-messaging/.

Coker, Margaret, Sam Schechner, and Alexis Flynn. "How Islamic State Teaches Tech Savvy to Evade Detection." *Wall Street Journal (Online)*, November 17, 2015., 1, *Academic Search Premier*, EBSCO*host.* Accessed April 14, 2016.

Collins, Hilton. “3 Technologies Claiming to Secure Messages in the Post-Snowden Era.” *Government Technology*. July 10, 2014. Accessed March 5, 2016. http://www.govtech.com/videos/3-Techs-Claim-to-Secure-Messages-in-the-Post-Snowden-Era.html.

Comey, James. “Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?” *Federal Bureau of Investigation*. October 16, 2014. Accessed March 28, 2016. https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

Comey, James. "Joint Statement with Deputy Attorney General Sally Quillian Yates Before the Senate Judiciary Committee." *Federal Bureau of Investigation*. July 8, 2015. Accessed March 9, 2016. https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy.

Comey, James. "Statement Before the Senate Select Committee on Intelligence." *Federal Bureau of Investigation*. July 8, 2015. Accessed March 9, 2016. https://www.fbi.gov/news/testimony/counterterrorism-counterintelligence-and-the-challenges-of-going-dark.

Cronk, Terri Moon. "Iraq Progresses in ISIL Fight, Key Extremist Confirmed Dead." U.S. *Department of Defense*. August 28, 2015. Accessed March 8, 2016. http://www.defense.gov/News-Article-View/Article/615305.

"Don't Panic: Making Progress on the "Going Dark" Debate." *Berkman Center for Internet & Society*. February 1, 2016. Accessed March 17, 2016. https://cyber.law.harvard.edu/publications/2016/Cybersecurity/Dont_Panic.

Duara, Nigel. "Man Tied to Cartoon Contest Attack Accessed Islamic State List, Authorities Say." *Los Angeles Times*. December 24, 2015. Accessed March 8, 2016. http://www.latimes.com/nation/la-na-garland-attack-20151224-story.html.

Duggan, Maeve. "Mobile Messaging and Social Media 2015." *Pew Research Center*. August 19, 2015. Accessed March 4, 2016. http://www.pewinternet.org/files/2015/08/Social-Media-Update-2015-FINAL2.pdf.

Eaton, Kit. "These Apps Promise to Encrypt Your Smartphone Communications." *The New York Times*. March 24, 2016. Accessed March 25, 2016. http://www.nytimes.com/2016/03/24/technology/personaltech/encryption-by-app-adds-security-to-smartphones.html?_r=0.

"Encryption." *Oxforddictionaries.com*. Accessed March 7, 2016. http://www.oxforddictionaries.com/us/definition/american_english/encryption.

Engel, Pamela. "A popular Messaging App Just Dealt a Potential Blow to ISIS." *Business Insider*. November 25, 2015. Accessed March 11, 2016. http://www.businessinsider.com/popular-messaging-app-telegram-just-dealt-a-potential-blow-to-isis-2015-11.

Engel, Pamela. "A Pro-ISIS Account is Giving its Belgian Followers Specific Instructions on How to Evade Authorities." *Business Insider*. March 22, 2016. Accessed March 23, 2016. http://www.businessinsider.com/isis-belgian-supporters-encryption-2016-3.

Engel, KeriLynn. “True Private Messaging: 7 Apps to Encrypt Your Chats.” *WhoIsHostingThis Blog*. April 29, 2015. Accessed March 5, 2016. http://www.whoishostingthis.com/blog/2015/04/29/im-encryption/.

Farivar, Cyrus. “From Encryption to Darknets: As Governments Snoop, Activists Fight Back.” *Ars Technica.* February 15, 2012. Accessed March 4, 2016. http://arstechnica.com/business/2012/02/from-encryption-to-darknets-as-governments-snoop-activists-fight-back/.

Fekete, Istvan. “iMessage Ranked ‘Moderately Safe’ by Islamic State, Telegram Preferred.” *iPhone in Canada*. November 18, 2015. Accessed March 11, 2016. http://www.iphoneincanada.ca/news/imessage-ranked-moderately-safe/.

Fingas, Roger. “Edward Snowden Hails Apple as ‘Pioneering’ for iOS 8 Security Measures.” *Apple Insider*. June 5, 2015. Accessed March 11, 2016. http://appleinsider.com/articles/15/06/05/edward-snowden-hails-apple-as-pioneering-for-ios-8-security-measures.

“From the National Security Agency.” *The New York Times*. January 27, 2014. Accessed March 9, 2016. http://www.nytimes.com/interactive/2014/01/28/world/28mobile-annotateA.html?_r=0.

Gadher, Dipesh. “British Hacker is No 3 on Pentagon ‘Kill List’.” *The Sunday Times*. August 2, 2015. Accessed March 8, 2016. http://www.thesundaytimes.co.uk/sto/news/uk_news/article1588418.ece.

Gellman, Barton, Andrea Peterson, and Ashkan Soltani. “How We Know The NSA Had Access to Internal Google and Yahoo Cloud Data.” *The Washington Post*. November 4, 2013. Accessed March 9, 2016. https://www.washingtonpost.com/news/the-switch/wp/2013/11/04/how-we-know-the-nsa-had-access-to-internal-google-and-yahoo-cloud-data/.

Gershgorn, Dave. “Apple Cares About Your Privacy, Unless You Use iCloud.” *Popular Science*. February 19, 2016. Accessed March 28, 2016. http://www.popsci.com/apple-cares-about-your-privacy-unless-you-use-icloud.

Gorta, Wiiliam J. “Garland Shooting: ‘Draw Muhammad’ Contest Host Pamela Geller Wants More, Similar Events.” *NBC News*. May 5, 2015. Accessed March 8, 2016. http://www.nbcnews.com/news/us-news/host-draw-muhammad-contest-says-must-be-more-similar-events-n353546.

Granville, Kevin. "9 Recent Cyberattacks Against Big Business." *The New York Times*. February 05, 2015. Accessed March 09, 2016. http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html?_r=0.

Grayson, Clary. "The Flaw in ISIS's Favorite Messaging App." *The Atlantic*. January 4, 2016. Accessed March 11, 2016. http://www.theatlantic.com/technology/archive/2016/01/isiss-favorite-messaging-app-has-a-security-problem/422460/.

Green, Matthew. "Here Come the Encryption Apps!" *A Few Thoughts on Cryptographic Engineering Blog*. March 9, 2013. Accessed February 29, 2016. http://blog.cryptographyengineering.com/2013/03/here-come-encryption-apps.html.

Greenwald, Glenn, Ewen MacAskill, Laura Poitras, Spencer Ackerman, and Dominic Rushe. "Microsoft Handed the NSA Access to Encrypted Messages." *The Guardian*. July 12, 2013. Accessed March 12, 2016. http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data.

Greenwald, Glenn. "NSA Prism Program Taps in to User Data of Apple, Google, and Others." *The Guardian*. June 7, 2013. Accessed March 7, 2013. http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

Gustin, Sam. "Google: We're No NSA Stooge and We'll Prove It if the Feds Let Us." *Time*. June 11, 2013. Accessed March 12, 2016. http://business.time.com/2013/06/11/google-were-no-nsa-stooge-and-well-prove-it-if-the-feds-let-us/.

Gustin, Sam. "Social Media Sparked, Accelerated Egypt's Revolutionary Fire." *Wired*. February 11, 2011. Accessed March 5, 2016. http://www.wired.com/2011/02/egypts-revolutionary-fire/.

Harbison, Cammy. "Microsoft Adds Enhanced Encryption To Outlook Email And Other Cloud Services, Increasing Privacy And Security." *iDigital Times*. July 2, 2014. Accessed March 7, 2016. http://www.idigitaltimes.com/microsoft-adds-enhanced-encryption-outlook-email-and-other-cloud-services-increasing-privacy-and.

Harris, Shane. "CIA's Ex-No. 2 Says ISIS 'Learned From Snowden'." *The Daily Beast*. May 6, 2015. Accessed March 11, 2016. http://www.thedailybeast.com/articles/2015/05/06/cia-s-ex-no-2-says-isis-learned-from-snowden.html.

Harris, Shane. "Your Samsung SmartTV Is Spying on You, Basically." *The Daily Beast*. February 5, 2015. Accessed March 22, 2016. http://www.thedailybeast.com/articles/2015/02/05/your-samsung-smarttv-is-spying-on-you-basically.html.

Hoffman-Andrews, Jacob. "Forward Secrecy at Twitter." *The Twitter Engineering Blog*. November 22, 2013. Accessed March 2, 2016. https://blog.twitter.com/2013/forward-secrecy-at-twitter-0.

"Hollande Calls Paris Attacks An 'Act of War'." *Al Jazeera*. November 14, 2015. Accessed March 10, 2016. http://www.aljazeera.com/news/2015/11/hollande-paris-france-attacks-concern-stadium-isil-151114103631610.html.

"Internet of Things Global Standards Initiative." *International Telecommunication Union*. Accessed March 21, 2016. http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx.

"I.S. Plot to Bomb UK Today." *The Sun*. June 26, 2015. Accessed March 7, 2016. http://www.thesun.co.uk/sol/homepage/news/6518366/Islamic-State-monster-aimed-to-kill-British-soldiers.html.

Joye, Christopher. "Interview Transcript: Former Head of the NSA and Command of the US Cyber Command, General Keith Alexander." *Financial Review*. May 8, 2014. Accessed March 7, 2016. http://www.afr.com/technology/web/security/interview-transcriptformer-head-of-the-nsa-and-commander-of-the-us-cyber-command-general-keith-alexander-20140507-itzhw.

Kaplan, Fred. "Sins of Omission." *Slate*. October 16, 2014. Accessed March 12, 2016. http://www.slate.com/articles/news_and_politics/war_stories/2014/10/citizenfour_review_laura_poitras_edward_snowden_documentary.html.

Kaplan, Rebecca. "Encrypted Messages: Does the Government Need a Way In?" *CBS News*. November 16, 2015. Accessed March 12, 2016. http://www.cbsnews.com/news/paris-attacks-encrypted-messages-does-the-government-need-a-way-in/.

Kaplan, Sarah. "Founder of App Used By ISIS Once Said 'We Shouldn't Feel Guilty.' On Wednesday He Banned Their Accounts." *The Washington Post*. November 19, 2015. Accessed March 9, 2016. https://www.washingtonpost.com/news/morning-mix/wp/2015/11/19/founder-of-app-used-by-isis-once-said-we-shouldnt-feel-guilty-on-wednesday-he-banned-their-accounts/.

Kelly, Samantha Murphy. “Samsung’s TVs Aren’t the Only Devices Listening to You.” *Mashable*. February 11, 2015. Accessed March 27, 2016. http://mashable.com/2015/02/10/smart-devices-listening/#N68IeFmGb5qX.

King, Meg, and Grayson Clary. “Opinion: The Shocking Mediocrity of Islamic State ‘Hacker’ Junaid Hussain.” *The Christian Science Monitor*. October 26, 2015. Accessed March 8, 2016. http://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/1026/Opinion-The-shocking-mediocrity-of-Islamic-State-hacker-Junaid-Hussain.

Kramer, Foster. “Twitter Buys Mobile Encryption Software, Weirdly Pulls It From Market, Basically Hates Egypt.” *Observer*. November 11, 2011. Accessed March 6, 2016. http://observer.com/2011/11/twitter-buys-mobile-encryption-software-weirdly-pulls-it-from-market-basically-hates-egypt/.

Lee, Timothy B. “NSA-Proof Encryption Exists. Why Doesn’t Anyone Use It?” *The Washington Post*. June 14, 2013. Accessed March 8, 2016. https://www.washingtonpost.com/news/wonk/wp/2013/06/14/nsa-proof-encryption-exists-why-doesnt-anyone-use-it/.

Liptak, Kevin. “Ex-counterterrorism Chief: U.S. Lost Track of Terrorists After Snowden.” *CNN*. October 21, 2014. Accessed March 11, 2016. http://www.cnn.com/2014/10/21/politics/olsen-nsa/index.html.

Madden, Mary, and Lee Rainie. “Americans’ Privacy Strategies Post-Snowden.” *Pew Research Center*. March 16, 2015. Accessed March 4, 2016. http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/.

Madden, Mary, and Rainie, Lee. “Americans’ Attitudes About Privacy, Security and Surveillance.” *Pew Research Center*. May 20, 2015. Accessed March 11, 2016. http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

Masnick, Mike. “Pissed Off Google Security Guys Issue FU To NSA, Announce Data Center Traffic Now Encrypted.” *TechDirt*. November 6, 2013. Accessed March 12, 2016. https://www.techdirt.com/articles/20131106/00235225143/pissed-off-google-security-guys-issue-fu-to-nsa-announce-data-center-traffic-now-encrypted.shtml.

McCaul, Michael, and Mark Warner. “How to Unite Privacy and Security – Before the Next Terrorist Attack.” *The Washington Post*. December 27, 2015. Accessed March 17, 2016. https://www.washingtonpost.com/opinions/how-to-unite-privacy-and-security--before-the-next-terrorist-attack/2015/12/27/628537c4-a9b3-11e5-9b92-dea7cd4b1a4d_story.html.

"McCaul, Warner Lead Bipartisan Coalition to Establish National Commission on Digital Security." *House Committee on Homeland Security*. February 29, 2016. Accessed March 17, 2016. https://homeland.house.gov/press/mccaul-warner-lead-bipartisan-coalition-to-establish-national-commission-on-digital-security/.

Mezzofiore, Gianluca. "Team Poison's Junaid Hussain Jailed for Tony Blair Hack and Phone Bombing Anti-Terror Hotline." *International Business Times*. July 27, 2013. Accessed March 8, 2016. http://www.ibtimes.co.uk/team-poison-phone-bomb-hacker-anti-terror-367660.

Miller, Christopher. "A Long Way From Moscow." *Mashable*. May 18, 2015. Accessed March 5, 2016. http://mashable.com/2015/05/18/russias-mark-zuckerberg-pavel-durov/#zr1.klvXSkq9.

Miller, Claire Cain. "Revelations of N.S.A Spying Cost U.S. Tech Companies. *The New York Times*. March 22, 2014. Accessed March 9, 2016. http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html?_r=1.

Mlot, Stephanie. "Only 6 Messaging Apps Are Truly Secure." *PC Magazine*. November 5, 2014. Accessed March 5, 2016. http://www.pcmag.com/article2/0,2817,2471658,00.asp.

Moody, Glyn. "Paris Terrorists Used Burner Phones, Not Encryption, To Evade Detection." *Ars Technica*. March 21, 2016. Accessed March 26, 2016. http://arstechnica.com/tech-policy/2016/03/paris-terrorist-attacks-burner-phones-not-encryption/.

Mortier, Richard. "Explainer: What is Perfect Forward Secrecy." *The Conversation*. December 2, 2013. Accessed March 2, 2016. http://theconversation.com/explainer-what-is-perfect-forward-secrecy-20863.

Munshani, Suni. "The Arab Spring of Privacy is Upon Us." *Wired*. November 7, 2014. Accessed March 9, 2016. http://www.wired.com/insights/2014/11/arab-spring-of-privacy/.

Murphy, Dan. "Inspired By Tunisia, Egypt's Protests Appear Unprecedented." *The Christian Science Monitor*. January 25, 2011. Accessed March 5, 2016. http://www.csmonitor.com/World/Backchannels/2011/0125/Inspired-by-Tunisia-Egypt-s-protests-appear-unprecedented.

Nakashima, Ellen, and Andrea Peterson. "Obama Administration Opts Not to Force Firms to Decrypt Data – for Now." *The Washington Post*. October 8, 2015. Accessed March 12, 2016. https://www.washingtonpost.com/world/national-security/obama-administration-opts-not-to-force-firms-to-decrypt-data--for-now/2015/10/08/1d6a6012-6dca-11e5-aa5b-f78a98956699_story.html.

Nakashima, Ellen. "Twitter Sues U.S. Government Over Limits on Ability to Disclose Surveillance Orders." *The Washington Post*. October 7, 2014. Accessed March 13, 2016. https://www.washingtonpost.com/world/national-security/twitter-sues-us-government-over-limits-on-ability-to-disclose-surveillance-orders/2014/10/07/5cc39ba0-4dd4-11e4-babe-e91da079cb8a_story.html.

National Information Standards Organization (NISO) (2004). *Understanding Metadata* (PDF). Bethesda, USA: NISO Press. ISBN 978-1-880124-62-8.

Palazzolo, Joe. "Apple Tells Court It Can't Unlock New iPhones." *The Wall Street Journal*. October 20, 2015. Accessed March 20, 2016. http://blogs.wsj.com/law/2015/10/20/apple-tells-court-it-cant-unlock-new-phones/.

"Paris Attacks: What Happened on the Night." *BBC News*. December 9, 2015. Accessed March 9, 2016. http://www.bbc.com/news/world-europe-34818994.

Perez, Evan, and Shimon Prokupecz. "First on CNN: Paris Attackers Likely Used Encrypted Apps, Officials Say." *CNN*. December 17, 2015. Accessed March 13, 2016. http://www.cnn.com/2015/12/17/politics/paris-attacks-terrorists-encryption/.

Pettersson, Edvard. "U.S. Drops Apple Case After Getting Into Terrorist's iPhone." *Bloomberg*. March 28, 2016. Accessed April 1, 2016. http://www.bloomberg.com/news/articles/2016-03-28/u-s-drops-apple-case-after-successfully-accessing-iphone-data-imcj88xu.

Pop, Valentina. "Belgium Warns of Terror Risk as Second Brussels Bombing Suspect Is Charged in Paris Attack." *The Wall Street Journal*. April 19, 2016. Accessed April 19, 2016. http://www.wsj.com/articles/belgium-still-at-risk-of-terror-attack-1461069025.

Porter, Tom. "Texas Shooting: ISIS Claims Responsibility for Attack on Mohammed Cartoons Contest." *International Business Times.* May 5, 2015. Accessed March 7, 2016. http://www.ibtimes.co.uk/texas-shooting-isis-claims-responsibility-attack-mohammed-cartoons-contest-1499685.

"Privacy Statement for Nest Products and Services." *Nest Labs*. March 10, 2016. Accessed March 22, 2016. https://nest.com/legal/privacy-statement-for-nest-products-and-services/.

Queally, Jon. "Anti-Muslim Event in Texas Ends in Gunfire, Two Deaths." *Common Dreams*. May 4, 2015. Accessed March 8, 2016. http://www.commondreams.org/news/2015/05/04/anti-muslim-event-texas-ends-gunfire-two-deaths.

Reitman, Janet. "Snowden and Greenwald: The Men Who Leaked the Secrets." *Rolling Stone*. December 4, 2013. Accessed March 11, 2016. http://www.rollingstone.com/politics/news/snowden-and-greenwald-the-men-who-leaked-the-secrets-20131204.

Saitta, Eleanor. "Can Encryption Save Us?" *Nation* 300, no. 24 (June 15, 2015): 16-18. *Academic Search Premier*, EBSCO*host.* Accessed February 29, 2016.

Sanger, David E., and Nicole Perlroth. "F.B.I. Chief Says Texas Gunman Used Encryption to Text Overseas Terrorist." *The New York Times*. December 9, 2015. Accessed March 9, 2016. http://www.nytimes.com/2015/12/10/us/politics/fbi-chief-says-texas-gunman-used-encryption-to-text-overseas-terrorist.html?_r=0.

Schechner, Sam, and Margaret Coker. "Telegram Messenger Blocks 78 Islamic State-Related Channels." *The Wall Street Journal*. November 18, 2015. Accessed March 11, 2016. http://www.wsj.com/articles/telegram-messenger-blocks-78-islamic-state-related-channels-1447897021.

Schmitt, Eric, and Ben Hubbard. "ISIS Leader Takes Steps to Ensure Group's Survival." *The New York Times.* July 21, 2015. Accessed February 29, 2016. http://www.nytimes.com/2015/07/21/world/middleeast/isis-strategies-include-lines-of-succession-and-deadly-ring-tones.html?_r=0.

"Secure Messaging Scorecard." *Electronic Frontier Foundation*. November 11, 2014. Accessed March 4, 2016. https://www.eff.org/secure-messaging-scorecard#about.

Shabtai, Paz. "Paris Attacks Raise Privacy Debate Once More." *iHLS*. November 20, 2015. Accessed March 5, 2016. http://i-hls.com/2015/11/paris-attacks-raise-privacy-debate-once-more/.

Shah, Reema. "Law Enforcement and Data Privacy: A Forward-Looking Approach." *Yale Law Journal* 125, no. 2 (November 2015): 543-558. *Academic Search Premier*, EBSCO*host*. Accessed February 28, 2016.

Shein, Esther. "Ephemeral Data." *Communications Of The ACM* 56, no. 9 (September 2013): 20-22. *Academic Search Premier*, EBSCO*host*. Accessed March 8, 2016.

Sorcher, Sara, and Malena Corollo. “Influencers: FBI Should Disclose San Bernadino iPhone Security Hole to Apple.” *The Christian Science Monitor*. March 24, 2016. Accessed March 26, 2016. http://www.csmonitor.com/World/Passcode/Passcode-Influencers/2016/0324/Influencers-FBI-should-disclose-San-Bernardino-iPhone-security-hole-to-Apple.

“Smartphone.” *Oxforddictionaries.com*. Accessed March 4, 2016. http://www.oxforddictionaries.com/us/definition/american_english/smartphone.

Spencer, Robert. "Allahu Akbar!!!!! 2 of our brothers just opened fire at the Prophet Muhammad (s.a.w) art exhibition in texas!” *Jihad Watch*. May 3, 2015. Accessed March 7, 2016. https://www.jihadwatch.org/2015/05/allahu-akbar-2-of-our-brothers-just-opened-fire-at-the-prophet-muhammad-s-a-w-art-exhibition-in-texas.

Spencer, Robert. “Garland Jihadi Sent 109 Encrypted Messages That FBI Can’t Read.” *Jihad Watch*. December 11, 2015. Accessed March 7, 2016. https://www.jihadwatch.org/2015/12/garland-jihadi-sent-109-encrypted-messages-that-fbi-cant-read.

Staten, James. “The Cost of PRISM Will Be Larger Than ITIF Projects.” *Forrester Research: James Staten’s Blog*. August 14, 2013. Accessed March 09, 2016. http://blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects

Stein, Letitia, and Colleen Jenkins. “Mohammad Cartoonist Says Police Killing of Two Gunmen ‘Justice’.” *Reuters*. May 4, 2015. Accessed March 7, 2016. http://www.reuters.com/article/us-usa-shooting-texas-cartoonist-idUSKBN0NP1ZS20150504.

Talev, Margaret, and Chris Strohm. “NSA Fallout Tests Obama Relationship With Tech Companies.” *Bloomberg*. December 18, 2013. Accessed March 12, 2016. http://www.bloomberg.com/news/articles/2013-12-18/nsa-fallout-tests-obama-relationship-with-tech-companies.

“Terms of Service.” *PC Magazine*. Accessed March 28, 2016. http://www.pcmag.com/encyclopedia/term/62682/terms-of-service.

“Top NYPD Official: ‘Technology Is Becoming A Big Enabler’ In Terrorists Secretly Planning Attacks.” *CBS New York*. March 22, 2016. Accessed March 23, 2016. http://newyork.cbslocal.com/2016/03/22/john-miller-nypd-brussels-attacks/.

US Congress. House. *To Establish in the Legislative Branch the National Commission on Security and Technology Challenges*, 114th Cong., 2d sess., H.R. 4651. https://homeland.house.gov/wp-content/uploads/2016/03/2016.03.03_HR-4651-Commission.pdf.

US Congress. Senate. *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy: Hearing before the Committee on the Judiciary*. 114th Cong., 1st sess., July 8, 2015. (statement of James B. Comey, Director, Federal Bureau of Investigation).

Vincent, James. "Telegram Messenger: App Built to Foil Russian Spies Soars After WhatsApp Trouble." *The Independent*. February 26, 2014. Accessed March 5, 2016. http://www.independent.co.uk/life-style/gadgets-and-tech/telegram-messenger-app-built-to-foil-russian-spies-soars-after-whatsapp-trouble-9154720.html.

Walter, Derek. "Why You Should Ditch SMS and Embrace Over-the-Top Messaging Apps." *Green Bot*. July 20, 2015. Accessed March 4, 2016. http://www.greenbot.com/article/2948898/android-apps/why-you-should-ditch-sms-and-embrace-over-the-top-messaging-apps.html.

"WhatsApp Encryption Shouldn't Be a Safe Haven to Cyber Criminals." *Hindustan Times*. April 7, 2016. Accessed April 8, 2016. http://www.hindustantimes.com/tech/whatsapp-encryption-shouldn-t-be-a-safe-haven-to-cyber-criminals/story-M1yBitHmkinvBdpaAhISgI.html.

Winton, Richard. "Why Brussels Attacks Exceeded San Bernadino's: A Terrorist Infrastructure." *Los Angeles Times*. March 22, 2016. Accessed March 25, 2016. http://www.latimes.com/local/lanow/la-me-ln-terrorist-infrastructure-brussels-vs-san-bernardino-20160322-story.html.

Winton, Richard. "San Bernadino Shooters Praised by Islamic State Magazine." *Los Angeles Times.* January 20, 2016. Accessed March 15, 2016. http://www.latimes.com/local/lanow/la-me-ln-islamic-state-magazine-san-bernardino-terrorists-20160120-story.html.

Wittes, Benjamin. "Jim Comey, ISIS, and "Going Dark"." *Lawfare Blog*. July 1, 2015. Accessed March 9, 2016. https://www.lawfareblog.com/jim-comey-isis-and-going-dark.

Yan, Holly. "Texas Attack: What We Know About Elton Simpson and Nadir Soofi." *CNN*. May 5, 2015. Accessed March 7, 2016. http://www.cnn.com/2015/05/05/us/texas-shooting-gunmen.

Youssef, Nancy A., and Amina Ismail. "Egypt's Second Twitter Revolution." *The Daily Beast*. December, 10, 2015. Accessed March 5, 2016. http://www.thedailybeast.com/articles/2015/12/11/egypt-s-second-twitter-revolution.html.

"#Terror Gone Viral: Overview of the 75 ISIS-Linked Plots Against the West 2014-2016." *House Homeland Security Committee*. March 2016. Accessed March 9, 2016. https://homeland.house.gov/wp-content/uploads/2016/03/Report-Terror-Gone-Viral-1.pdf.