CRYPTO WARS 2.0: WHY LISTENING TO APPLE ON ENCRYPTION WILL MAKE AMERICA MORE SECURE

*By: Paul McLaughlin**

I. INTRODUCTION

Encryption is a topic that has garnered significant attention in the United States (U.S.) because of the controversy between the Federal Bureau of Investigation (FBI) and Apple.[1] A federal magistrate judge initially ordered Apple to comply with the FBI's request that Apple break into the encrypted phone of a perpetrator of the San Bernardino terrorist attack on December 2, 2015.[2] Apple resisted this order, going so far as to release a public letter explaining its reasons why.[3] As per a Government Status Report filed on March 28, 2016, the FBI successfully accessed the phone in question without the assistance of Apple.[4]

There is much debate over the role that encryption plays in the war on terror writ large, with the increased use of the Telegram application by the terrorist group known as the "Islamic State of Iraq and the Levant" (ISIS).[5] Many Internet companies have recently moved to end-to-end encryption for messaging systems, which provides greater user privacy.[6] In addition, many smartphone manufacturers

---

*J.D., Temple University Beasley School of Law, 2016. I would like to thank Associate Dean Duncan Hollis for his feedback and guidance throughout writing this, as well as the Editorial Board and Staff Editors that have improved this article throughout the last year. I also want to thank my family and friends for their patience and support throughout law school. Lastly, thank you Liz, for your encouragement to write this, and for everything.

1. *See* Anusha Asif, *Apple vs. FBI: Encryption Case Timeline*, TECH NEWS TODAY.COM (Feb. 29, 2016, 7:07 AM), http://www.technewstoday.com/28773-apple-vs-fbi-encryption-case-timeline/ (discussing the controversy between Apple and the FBI, where the FBI attempted to enforce a court order forcing Apple to de-encrypt the phone owned by one of the shooters who committed a mass shooting and attempted bombing in San Bernadino, California).

2. *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. ED 15–0451M (C.D. Cal. Feb. 16, 2016).

3. Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), http://www.apple.com/customer-letter/.

4. Alina Selyukh, *The FBI Has Successfully Unlocked the iPhone Without Apple's Help*, NPR (Mar. 28, 2016, 6:20 PM), http://www.npr.org/sections/thetwo-way/2016/03/28/472192080/the-fbi-has-successfully-unlocked-the-iphone-without-apples-help.

5. Telegram is a messaging and social networking application allowing users a wealth of options, including state-of –the-art encryption, a relatively private tool for dissemination to large groups, and which is, most importantly, free. Jamie Dettmer, *Why Islamic State Loves Telegram*, VOICE OF AMERICA (Jan. 8, 2008, 1:55 PM), http://www.voanews.com/content/why-islamic-state-loves-telegram/3137040.html. There are many different names for the group ISIS. Faisal Irshaid, *Isis, Isil, IS or D'aesh? One Group, Many Names*, BBC NEWS (Dec. 2, 2015), http://www.bbc.com/news/world-middle-east-27994277. For the purpose of this comment, the group is referred to as ISIS, unless called ISIL or D'aesh by the source referenced.

6. *See* Harold Abelson et al., *Keys Under Doormats: Mandating Insecurity by Requiring*

are creating operating systems for their devices that render information stored on the devices encrypted by default.[7] Digital encryption is a way of coding plaintext so that only the receiver of a message or information can "break the code."[8] But do more secure systems make us more vulnerable or do they make us safer? Furthermore, who gets to decide the norms of encryption? When Apple and Microsoft and Google are operating all over the globe, does the U.S. get to decide how communications are passed across these global networks?

Public confusion over the use of encryption technology and heavy-handed regulation by foreign states will make our communications systems more vulnerable,[9] and by extension, less safe. The tech industry takes the position that it is not feasible to provide law enforcement agencies with a golden key to access encrypted information.[10] They argue that compromising encryption even in the slightest would leave an opening for bad actors, whether they are hostile states, domestic hackers, or terrorist networks. U.S. policymakers, however, argue that there must be ways to access encrypted information to combat domestic and international terrorism. After the San Bernadino attacks, *Apple v. FBI*[11] served as a watershed moment in the regulation of encrypted information in the U.S. and the understanding of what is at stake by the imposition of "backdoors."[12]

This comment begins with a brief synopsis on the technology involved in end-to-end encryption and its current uses. The comment then moves to a survey of the four main viewpoints on the utility of end-to-end encryption. This comment

---

Government Access to All Data and Communications, COMPUTER SCIENCE & ARTIFICIAL INTELLIGENCE 11 (July 6, 2015) (examining the use of encryption in popular social media platforms today); *see infra* Section II (further defining public and private keys).

7. *See infra* Section II (examining the use of encryption in popular social media platforms today).

8. *See* Abelson et al., *supra* note 6, at 11 (explaining that transformed data was protected by a symmetric key that operates in a mode where the sent data was encrypted and can only be accessed by the receiver); *see also Plain text*, WEBOPEDIA, http://www.webopedia.com/TERM/P/plain_text.html (last visited Oct. 23, 2016) ("In cryptography, plain text refers to any message that is not encrypted."). Plain text, plain-text, or plaintext is also used to refer to any text that contains only text and does not support formatting, including basic formatting such as italicization. *Plain text*, COMPUTER HOPE, http://www.computerhope.com/jargon/p/plaintex.htm (last visited Oct. 23, 2016).

9. *See* Shangyong Mima Guanli Tiaoli (商用密码管理条例) [Regulation of Commercial Encryption Codes] (promulgated by the State Council, Directive No. 273, Oct. 7, 1999, effective Oct. 7, 1999) http://newmedia.cityu.edu.hk/cyberlaw/gp3/pdf/law_encryption.pdf (China) (creating a system which makes it easier for the government to access encrypted communications through monopoly of Wi-Fi devices, making U.S. assets stationed in China potentially more vulnerable).

10. Amul Kalia, *Where Do the Major Tech Companies Stand on Encryption?*, ELEC. FRONTIER FOUND. (Oct. 9, 2015), https://www.eff.org/deeplinks/2015/10/where-do-major-tech-companies-stand-encryption.

11. *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. ED 15–0451M (C.D. Cal. Feb. 16, 2016).

12. *See* Kalia, *supra* note 10 (arguing that the government intended to enforce backdoors, an extra-legal process, to attempt to obtain user data from technology companies).

discusses the positions taken by those in the tech industry and argues that the majority position of those in the tech industry—that strong encryption makes systems less susceptible to hacking and cyber-attack—is the best position. Making our current encrypted systems vulnerable to any degree will open the door for hackers and hostile nations to exploit the vulnerabilities.[13] Deferring to the positions of the tech industry while other countries make their systems more vulnerable will ultimately help make the U.S. safer from terrorism.

II. BACKGROUND ON ENCRYPTION

End-to-end encryption is a method of coding information that is sent from one user to another user, or a group of users.[14] There are two types of basic encryption methods: public key and private key.[15] Keys are devices or algorithms used to encode or decode messages.[16]

Public key encryption involves a public key and a private key.[17] A sender encodes a message using his private key that would then be decoded by the recipient's public key, or vice versa.[18] On the other hand, private key encryption involves only one key, the private key.[19] The sender sends the key along with the message and it is used to decode the message.[20] Private key encryption is the less secure of the two methods of encryption because the key travels with the message.[21]

The majority of usage of end-to-end encryption technology is for benign purposes such as to facilitate online banking and shopping.[22] Technology (tech) companies have moved to more secure encryption technology to bolster individual privacy, and arguably to bolster their bottom line.[23]

There is growing debate over the use of encryption technology by terrorist

---

13. *Id*.

14. *See Encryption Tech, and Possible US Policy Responses: Hearing Before H.R. Comm. on Gov't Oversight and Reform Info. Tech. Subcomm.*, 114th Cong. 4 (2015) (statement of Matt Blaze) [hereinafter *U.S. H.R. Statement of Matt Blaze*) (explaining that the end-to-end encryption is conducted entirely between communicating parties).

15. Kurt M. Saunders, *The Regulation of Internet Encryption Technologies: Separating the Wheat from the Chaff*, 17 J. MARSHALL J. COMPUTER & INFO. L. 945, 948 (1999).

16. *U.S. H.R. Statement of Matt Blaze*, *supra* note 14, at 4.

17. Saunders, *supra* note 15, at 948.

18. *Id*.

19. *Id*.

20. *Id*.

21. *Id*. Public key encryption can also generate digital signatures, which authenticate the identity of the sender of a message and also make the content of the message available. *Id*. at 948–949.

22. Charles Arthur, *How Internet Encryption Works*, GUARDIAN (Sept. 5, 2013, 3:19 PM), https://www.theguardian.com/technology/2013/sep/05/how-internet-encryption-works.

23. *See* Joe Ross, *2015: The Plague of Point-of-Sale Breaches Continues*, INT'L ASS'N OF PRIVACY PROF'LS (Apr. 28, 2015), https://iapp.org/news/a/2015-the-plague-of-point-of-sale-breaches-continues/ (describing a combination of PIN protection and EMV cards developed by tech companies to bolster more privacy for their users).

organizations. For example, some argue that terrorist groups used encryption technology to plan two recent terrorist attacks in Paris, France and San Bernadino, California.[24] On November 13, 2015, in Paris, France, three suicide bombers struck outside the Stade de France, while simultaneous mass shootings were taking place at cafés, restaurants, and inside the Bataclan theatre,[25] during which 368 people were injured and 130 people died.[26] Officials speculated that encrypted applications (apps) such as Telegram and WhatsApp were used to plan these attacks.[27]

On December 2, 2015, in San Bernardino, California, two individuals killed fourteen people and seriously injured twenty-two more in a terrorist attack targeted at an office holiday party.[28] An encrypted iPhone owned by one of the perpetrators became the focal point for the controversy between the FBI and Apple over encryption and the authority of the federal government to force private companies to comply with U.S. security directives.[29]

The increased use of encryption for both individual privacy and potential terrorist use raises the question of whether or not the increased use of more secure encryption systems makes the world safer or more vulnerable to terrorist activities and other attacks. Several major tech companies have encryption already built into their messaging systems.[30] Many email systems or email chat systems use a form of

---

24. *Compare* Michael Birnbaum, Souad Mekhennet, & Ellen Nakashima, *Paris Attack Planners Used Encrypted Apps, Investigators Believe*, WASH. POST (Dec. 17, 2015), https://www.washingtonpost.com/world/europe/paris-attack-planners-used-encrypted-apps-investigators-believe/2015/12/17/e798d288-a4de-11e5-8318-bd8caed8c588_story.html (representing the belief that encrypted technology was used in the attack and indicating that because the terrorists used widely available encryption tools to communicate with each other, it was difficult for investigators to monitor their conversations), *with* Jeff Larson & Julia Angwin, *Fact Checking the Debate on Encryption*, PROPUBLICA (Dec. 15, 2015), https://www.propublica.org/article/fact-checking-the-debate-on-encryption (placing the possible use of an encrypted telephone by one of the Paris attackers in a larger context).

25. *See* Eleanor Steafel et al., *Paris Terror Attack: Everything We Know on Saturday Afternoon*, THE TELEGRAPH (Nov. 21, 2015, 4:30 PM), http://www.telegraph.co.uk/news/worldnews/europe/france/11995246/Paris-shooting-What-we-know-so-far.html (giving a timeline of the attacks in Paris).

26. *See id*. (stating that 130 people were killed); *see also* Adam Chandler, Krishnadev Calamur, & Matt Ford, *The Paris Attacks: The Latest*, THE ATLANTIC (Nov. 22, 2015), http://www.theatlantic.com/international/archive/2015/11/paris-attacks/415953/ (stating that 368 people were injured).

27. Evan Perez and Shimon Prokupecz, *First on CNN: Paris Attackers Likely Used Encrypted Apps, Officials Say*, CNN (Dec. 17, 2015, 10:00 AM), http://www.cnn.com/2015/12/17/politics/paris-attacks-terrorists-encryption/.

28. Sarah Parvini, *For Those Wounded in San Bernadino, a Painful Path to Recovery*, LOS ANGELES TIMES (Dec. 30, 2015, 5:00 AM), http://www.latimes.com/local/california/la-me-sb-victim-recovery-20151230-story.html.

29. *See* Ellen Nakashima, *Apple Vows to Resist FBI Demand to Crack iPhone Linked to San Bernadino Attacks*, WASH. POST (Feb. 17, 2016), https://www.washingtonpost.com/worldnational-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardinoshooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html (explaining the controversy between Apple and the FBI over an iPhone used by one of the San Bernadino shooters).

30. *See* John E. Dunn, *The Best Secure Mobile Messaging Apps 2016*, TECH WORLD (Nov. 8, 2015), http://www.techworld.com/security/best-secure-mobile-messaging-apps-2015-3629914/

encryption.[31] The most common and respected form of encryption is "Pretty Good Privacy" (PGP).[32] The founder of PGP, Phil Zimmermann, also called the "King of Encryption," created PGP in the early 1990s.[33] Mr. Zimmermann initially distributed PGP for free to any Internet user that desired to use it.[34]

True end-to-end encryption hides the content of a transmission of information from even the administrators of the application used (e.g., Apple, Facebook, etc.).[35] End-to-end encryption is growing in popularity within the tech field due to its high degree of privacy. For example, Google is seeking to release "End-to-End," a Chrome plug-in that encrypts messages end-to end.[36] Facebook has also made its own "Dark Web" website,[37] acquired WhatsApp, a messaging company that uses

---

(identifying multiple messaging systems best used for encrypted messaging, including Telegram, Signal, and Pryvate).

31. *Email Encryption: A Security Necessity*, ENCRYPTOMATIC, https://www.encryptomatic.com/emailsecurity/email-encryption-systems.html (last visited Oct. 20, 2016).

32. Juliette Garside, *Phil Zimmermann: King of Encryption, Reveals His Fears for Privacy*, GUARDIAN (May 25, 2015, 12:02 PM), http://www.theguardian.com/technology/2015/may/25/philip-zimmermann-king-encryption-reveals-fears-privacy.

33. *Id*.

34. *Id*.

35. *See* Asif, *supra* note 1 (recognizing that no "backdoor" exists for Apple's product and therefore administrators needed to create one to see encrypted information).

36. Frederic Lardinois, *Google's End-to-End Encryption Tool Gets Closer to Launch*, TECHCRUNCH (Dec. 17, 2014), http://techcrunch.com/2014/12/17/googles-end-to-end-email-encryption-tool-gets-closer-to-launch/.

37. *See* Andy Greenberg, *Hacker Lexicon: What Is the Dark Web*, WIRED (Nov. 19, 2014, 7:15 AM), http://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/ ("Even Facebook has launched a Dark Web site aimed at better catering to users who visit the site using Tor to evade surveillance and censorship"). Tor and the Dark Web are very complex issues, so this will be a relatively basic explanation of both. Based out of a nonprofit that does research and development into Internet privacy, Tor offers a technology that bounces users' and websites' traffic through thousands of "relays" provided by volunteers across the globe. This makes tracking the source of the information or the location of the user difficult. Tor was originally created by the U.S. Navy and received much of its initial funding from the State Department. *Tor: Overview*, TOR PROJECT, https://www.torproject.org/about/overview (last visited Oct. 20, 2016). Tor is mainly used for lawful purposes by five different groups: (1) normal people who want to keep their internet activities private from websites and advertisers, (2) those concerned about cyberspying, (3) users evading censorship present in their part of the world, (4) military personnel, and (5) activists and journalists evading censorship. Tor is also used by criminals and terrorists across the world to maintain anonymity. Criminal users use Tor and similar anonymity networks on what is called the "Dark Web". *See Who Uses Tor?*, TOR PROJECT, https://www.torproject.org/about/torusers.html (last visited Oct. 20, 2016) (describing different groups that use Tor as well as their objectives). The Dark Web is a subset of the Deep Web, which is essentially the area search engines cannot crawl for or index. The Dark Web and the Deep Web are terms that are often used interchangeably. *Clearing Up Confusion – Deep Web vs. Dark Web*, BRIGHTPLANET (Mar. 27, 2014), https://brightplanet.com/2014/03/clearing-confusion-deep-web-vs-dark-web/. For purposes of this comment, though, the Deep Web is the larger entity that includes the Dark Web as one of its parts. The Dark Web is an area within the Deep Web that is intentionally hidden from discovery. Charlie Osborne, *10 Things You Didn't Know about the Dark Web*, ZDNET (Oct. 15, 2015), http://www.zdnet.com/pictures/10-things-you-didnt-know-about-the-dark-web/. Users

end-to-end encryption in its Android application,[38] and launched features that enabled users to get notifications through encrypted emails.[39] Facebook appears to be moving in the direction of more encryption in its capabilities.[40]

III. THE MAIN VIEWPOINTS ON THE DEBATE OVER ENCRYPTION

There are four main viewpoints surrounding the current debate over encryption. The first is that secure networks actually make us safer.[41] The second is that completely secure networks force law enforcement and anti-terror groups to operate at an unacceptable handicap.[42] The third viewpoint, which is somewhere in between, is that secure systems generally make us safer, but that exceptional access should be available in certain situations.[43] Fourth, according to David Chaum, encryption in its purest form is not the optimal way of ensuring privacy and security, but rather encryption should be a part of a larger privacy scheme.[44]

---

generally access the Dark Web through the Tor network or a similar anonymity network. The Dark Web utilizes onion domains, which maintain low-latency communication, in order to resist surveillance and traffic analysis. The Dark Web has been home to illicit drug markets like the infamous Silk Road marketplace, as well as markets for pornography, weapons, and hitmen. *Buying Drugs Online: Shedding Light on the Dark Web*, ECONOMIST (July 16, 2016), http://www.economist.com/news/international/21702176-drug-trade-moving-street-online-crypto markets-forced-compete. It is also home to message boards on topics like political activism and hacking. Benjamin Vitáris, *Anonymous Teaches Hacking on Dark Web Chat Network*, DEEP.DOT.WEB (May 7, 2016), https://www.deepdotweb.com/2016/05/07/anonymous-teaches-hacking-dark-web-chat-network/. Finally, most purchases that take place on the dark web utilize Bitcoin, a popular cryptocurrency. Jake Rocheleau, *Introduction to Bitcoins and the Tor Network*, HONGKIAT, http://www.hongkiat.com/blog/introductions-to-bitcoins-tor-network (last visited Oct. 20, 2016).

38. There is debate on the integrity of the end-to-end encryption used by WhatsApp. An employee of the Dutch Intelligence Service AIVD, speaking during a seminar marking the AIVD's 70th anniversary, stated that "I would not trust that WhatsApp is so safe." Janene Pieters, *Dutch Intelligence Service Warns of WhatsApp Security Issue*, NLTIMES.NL (Nov. 6, 2015, 12:27 PM), http://www.nltimes.nl/2015/11/06/dutch-intelligence-service-warns-of-whatsapp-security-issue/. This was in response to a question regarding whether or not AIVD officers could read communications taking place over WhatsApp. *Id*.

39. Klint Finley, *New Facebook Feature Shows Actual Respect for Your Privacy*, WIRED (June 1, 2015, 5:42 PM), http://www.wired.com/2015/06/new-facebook-feature-shows-actual-respect-privacy/.

40. *See id*. (discussing Facebook's attempt to strengthen users' privacy by incorporating encryption into their service, including the encryption of email notifications sent by Facebook).

41. *See infra* Part IV (discussing the position of major tech industries of allowing a special key to break encryption).

42. *See infra* Part VI (discussing the aftereffects of the watershed controversy between Apple and the FBI).

43. *See infra* Section VI.C.2 (arguing that only certain government agencies in certain nation states should have access to encrypted communications and largely only in exceptional situations).

44. Andy Greenberg, *The Father of Online Anonymity Has a Plan to End the Crypto War*, WIRED (Jan. 6, 2016, 7:00 AM), http://www.wired.com/2016/01/david-chaum-father-of-online-anonymity-plan-to-end-the-crypto-wars/. David Chaum is the inventor of many encryption protocols and founder of the International Association for Cryptologic Research (IACR). His idea would work practically as a smartphone application. The application, still in its beta testing, is

The tech industry generally holds the first viewpoint that completely secure networks make us safer.[45] Those in the tech commentary community also widely believe in completely secure networks.[46] Additionally, the Netherlands has stated this to be their national policy on regulating encryption.[47] This viewpoint is rooted in the belief that allowing national actors to have exceptional access would create vulnerabilities that bad actors would exploit.[48] Adherents to this viewpoint generally oppose government access on principle[49] or out of practicality.[50]

Law enforcement agencies around the world hold the second viewpoint that embracing full encryption presents an unacceptable risk.[51] Tech and computer security commentators, as well as governments of certain nations, also adhere to the view that some access to encrypted information is needed.[52] Advocates of this viewpoint emphasize findings regarding the use of encrypted devices by terrorist groups and dangerous criminals to support their view.[53] They argue that allowing

---

meant by Chaum to be more secure and anonymous than the Tor Network. However, it would have an intentional backdoor that would allow for the privacy and anonymity to be removed from someone "generally recognized as evil." *Id*. The insurance for the security of the system comes from the backdoor being divided amongst many key-holders in many different and diverging jurisdictions. *Id*.

45. *See infra* Part IV (discussing the position of major tech industries of allowing a special key to break encryption).

46. *Id*.

47. *See* Section V.G (explaining that the Netherlands would not mandate any encryption backdoors because of the belief that a strongly encrypted Internet was in the country's best interest).

48. Sarah Jeong, *A 'Golden Key' for Encryption is Mythical Nonsense*, MOTHERBOARD (July 21, 2015, 8:45 AM), http://motherboard.vice.com/read/a-golden-key-for-encryption-is-mythical-nonsense.

49. *See* Cook, *supra* note 3 (stating the necessity of encryption as well as Apple's opposition to government regulation because of the threat on data security and personal safety).

50. *See* David E. Sanger & Nicole Perlroth, *Encrypted Messaging Apps Face New Scrutiny over Possible Role in Paris Attacks*, N.Y. TIMES (Nov. 16, 2015), http://www.nytimes.com/2015/11/17/world/europe/encrypted-messaging-apps-face-new-scrutiny-over-possible-role-in-paris-attacks.html (referencing Bill Bratton's argument that much of the tech industry's posturing over this issue has been a matter of marketing).

51. Cyrus R. Vance Jr., François Molins, Adrian Leppard, & Javier Zaragoza, *When Phone Encryption Blocks Justice*¸ N.Y. TIMES (Aug. 11, 2015), http://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html.

52. *See, e.g*., Benjamin Wittes, *Thoughts on Encryption and Going Dark, Part II: The Debate on the Merits*, LAWFARE BLOG (July 12, 2015), https://www.lawfareblog.com/thoughts-encryption-and-going-dark-part-ii-debate-merits; *see also* Editorial Board, *Putting the digital keys to unlock data out of reach of authorities*, WASH. POST (July 18, 2015), https://www.washingtonpost.com/opinions/putting-the-digital-keys-to-unlock-data-out-of-reach-ofauthorities/2015/07/18/d6aa7970-2beb-11e5-a250-42bd812efc09_story.html (discussing the editorial about the dangers of full encryption and the balance needed between law enforcement and the tech industry) [hereinafter Editorial Board]; *see infra* Sections V.A.–D (explaining that the governments of the UK, the People's Republic of China, France, and India have each come up with their own policies in regard to regulation of encryption technologies).

53. *See* Jenna McLaughlin, *FBI and Comey Find New Bogeyman for Anti-Encryption Arguments: ISIS*, INTERCEPT (July 7, 2015, 2:36 PM), https://theintercept.com/2015/07/07/fbi-

full encryption allows these bad actors to have an advantage over law enforcement.[54] This viewpoint recognizes the benefit of government access to these communications, and that increased access is worth the accompanying privacy risks associated with less secure and more vulnerable systems.[55]

The American national security apparatus holds the third viewpoint, which states that secure systems generally make us safer, but access in certain circumstances is necessary.[56] National Security Agency (NSA) Director Michael S. Rogers best summarized this view: "I don't want a back door . . . I want a front door. And I want the front door to have multiple locks. Big locks."[57] Adherents to this viewpoint argue that only certain government agencies in certain nation states should have exceptional access to encrypted communications.[58]

The fourth viewpoint, advocated by encryption pioneer David Chaum, asserts that encryption can be part of a larger privacy scheme, but that it should not be the final arbiter of what is private and what is secure.[59] Mr. Chaum has been creating "PrivaTegrity," an encryption system that allows for "fully secret, anonymous communications" with a special backdoor controlled by a "council."[60] Chaum's system is not a pure end-to-end encryption but is a unique solution to a stalemate over privacy.[61]

IV. THE DOMINANT POSITION OF THE TECH INDUSTRY

The majority, if not nearly all, of the big tech companies believe that end-to-end encryption is necessary to protect user data.[62] Tech companies also believe that having encrypted systems with a "special key" or access for government and law

finds-new-bogeyman-anti-encryption-arguments-isis/ (quoting FBI Director Comey's argument that ISIS does most of its planning through mobile messaging applications).

54. *See* Vance et al., *supra* note 51 (citing to chief prosecutors from multiple major international jurisdictions).

55. *Id*.

56. *See infra* Section VI.C.1 (further discussing the view that secure systems are safer, but access is sometimes necessary).

57. Ellen Nakashima & Barton Gellman, *As Encryption Spreads, U.S. Grapples with Clash Between Privacy, Security*, WASH. POST (Apr. 10, 2015), https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html.

58. *See id.* ("Countries including the United Kingdom, Australia, and China have passed or are contemplating laws seeking government access to communications similar to that sought by U.S. authorities."); *see also* Nicole Perlroth, *Security Experts Oppose Government Access to Encrypted Communication*, N.Y. TIMES (July 7, 2015) (discussing the government proposal for "exceptional access" to encrypted data).

59. Greenberg, *supra* note 44.

60. *Id*.

61. *Id*.

62. *See* Sophie Curtis, *Wikipedia Founder Urges Apple to Stop Selling iPhones in UK If Government Bans Encryption*, TELEGRAPH (Nov. 4, 2015, 1: 29 AM), http://www.telegraph.co.uk/technology/jimmy-wales/11974687/Wikipedia-Founder-urges-Apple-to-stop-selling-iPhones-in-UK-if-government-bans-encryption.html (indicating that Apple, Facebook, Snapchat, WhatsApp, Google, and other communication providers use end-to-end encryption to protect user data).

enforcement is not technically feasible because it is costly to protect.[63] According to the industry and surrounding commentaries, the assumption is that seeking to carve out special access for law enforcement is based on a lack of understanding of the technology involved in encryption.[64]

There are three likely explanations to the tech industry's position on limiting access to governments and law enforcement on encryption technology. First, leaders of the large tech companies genuinely value individual privacy.[65] Second, large tech companies genuinely think that the Internet will be the most secure—and thus our society the safest—with full encryption.[66] Third, large tech companies believe that privacy is a good sales strategy that will increase their bottom line.[67]

On the basis of preserving individual privacy and the belief that any "backdoor" or special access to data for law enforcement would make the world less secure, large tech companies have also staunchly fought back against government efforts to access their encrypted technology. For example, in 2015, the United Kingdom (U.K.) introduced a draft Investigatory Powers Bill.[68] The bill required big tech companies to decrypt communications on the companies' devices on demand as well as retain their users' browser histories for a year so that the U.K. could have access to such information if needed for law enforcement purposes.[69] Apple released statements opposing the legislation.[70] Apple CEO Tim Cook made several public statements opposing the bill, stating, "If you close down the major companies from using encryption, the bad guys aren't going to stop using encryption. They are just going to go to another source."[71] Cook also asserted, "If you leave a back door in the software, there is no such thing as a back

63. *See* Abelson et al., *supra* note 6 (concluding that costs associated with creating a special key would be substantial and greatly damage innovation); *see also* Asif, *supra* note 1 (discussing Apple's refusal to create a backdoor key for use by the FBI).

64. *See* Curtis, *supra* note 62 (providing a quote from Nigel Hawthorn, a spokesperson for a cloud security company, indicating that the government misunderstands how end-to-end encryption works).

65. Cook, *supra* note 3; *see also* Editorial Board, *supra* note 52 (indicating that hardware and software industry associations are opposed to measures that would undermine encryption technology).

66. *See* Nakashima & Gellman, *supra* note 57 (discussing how Yahoo's chief of information security believes that law enforcement is requesting security vulnerabilities that hackers and foreign spy agencies could exploit).

67. *See* Cook, *supra* note 3 (explaining customer expectation of privacy and protection in technology products); *see also* Chris Smith, *New U.K. Law Might Force Apple to Decrypt the iPhone for Police Investigations*, BGR (Nov. 3, 2015, 10:00 PM), http://bgr.com/2015/11/03/iphone-encryption-u-k-law/ ("These companies' reputations rest on their ability to protect their users' data.").

68. Smith, *supra* note 67.

69. *Id*.

70. Conor Humphries, *Apple Says against Opening Encrypted Data for Britain*, REUTERS (Nov. 11, 2015, 12:19 PM), http://www.reuters.com/article/us-britain-security-apple-idUSKCN0T022Z20151111.

71. *Id*.

door for good guys only. . . . If there is a back door, anyone can come in the back door."[72]

In the wake of the *Apple v. FBI* controversy that unfolded in the spring of 2016 in the U.S., Apple also released statements with equally strident language.[73] Apple's customer letter, within the subheading "Need for Encryption," contained the following passage:

> All that information needs to be protected from hackers and criminals who want to access it, steal it, and use it without our knowledge or permission. Customers expect Apple and other technology companies to do everything in our power to protect their personal information, and at Apple we are deeply committed to safeguarding their data. Compromising the security of our personal information can ultimately put our personal safety at risk. That is why encryption has become so important to all of us. For many years, we have used encryption to protect our customers' personal data because we believe it's the only way to keep their information safe. We have even put that data out of our own reach, because we believe the contents of your iPhone are none of our business.[74]

Members of the tech industry commentariat have also decried government efforts to create secure encryption keys.[75]

Additionally, the Massachusetts Institute of Technology released a 2015 report on end-to-end encryption and the risks of government access titled *Keys Under Doormats*.[76] The report was written by fifteen computer science and security experts[77] and is perhaps one of the most comprehensive analyses performed on this subject to date. The experts argued that the price of granting law enforcement exceptional access to user privacy would be more damaging today than it would have been twenty years ago, referring to the Clipper Chip controversy of the 1990s.[78]

However, not all tech commentators or the general media are in support of end-to-end encryption. A July 18, 2015 editorial by the Editorial Board of the Washington Post requested that Congress heed the points of both sides of the debate when fashioning policy.[79] The Editorial Board discussed a set of possible limits for Internet freedom centered on the "legitimate needs of U.S. law

---

72. *Id*. This position has been seconded by Nigel Hawthorn, spokesperson for cloud-based security company Skyhigh Networks: "'There's a complete misunderstanding of how end-to-end encryption works. It's wrong to assume that forcing technology companies to break their own security is going to please the average man on the street, and this is not even technically possible in many instances . . . despite the inevitable backlash from technology experts, politicians continue to announce these ill-thought-out unworkable proposals.'" Curtis, *supra* note 62.

73. *See, e.g.*, Cook, *supra* note 3.

74. *Id*.

75. Jeong, *supra* note 48.

76. Abelson et al., *supra* note 6.

77. *Id*.

78. *Id*. For more information about the Clipper Chip controversy see infra Section VI.B.

79. Editorial Board, *supra* note 52.

enforcement."[80] The Board also stated that it believes that the Internet should "be subject to the same rule of law and protections that we accept for the rest of society."[81]

V. THE GLOBAL BATTLE OVER THE REGULATION OF ENCRYPTION

There does not seem to be a strong correlation between the type of government and the degree of regulation on encryption technology. For example, one of the nations that is proposing one of the strongest sets of regulations is the UK, a country not known in recent history for being authoritarian in its surveillance of its own citizens. Notably, the countries that have typically been known for their libertarian ideals, such as the U.S. and the Netherlands, have wrestled more with the correct course of action.

It appears that the most common thread in the debate over how to regulate encryption is tied to a country's recent experiences with terrorist attacks. Countries where terror has become a larger concern, such as the U.S.,[82] China,[83] and France,[84] have either passed stringent regulations or have debated stringent regulations regarding encryption in recent years.[85] Conversely, countries surveyed that have not experienced terrorism in recent years have utilized more traditional methods of surveillance to combat Internet crime.[86]

The following sub-sections discuss differing legislative positions and commentaries from the U.K., China, South Korea and India. The countries are presented by level of government access, from most government access to the least. Following these is a brief discussion of the use of encryption by ISIS, which is the greatest international terrorist concern for countries currently addressing regulation of encrypted information.[87]

A. The United Kingdom

As discussed in Section IV above, the U.K. introduced the draft Investigatory

---

80. *Id*.

81. *Id*.

82. Alina Selyukh & Steve Henn, *After Paris Attacks, Encrypted Communication Is Back in Spotlight*, NPR ALL TECH CONSIDERED (Nov. 16, 2015, 5:29 PM), http://www.npr.org/sections/alltechconsidered/2015/11/16/456219061/after-paris-attacks-encrypted-communication-is-back-in-spotlight.

83. Scott D. Livingston, *Will China's New Anti-Terrorism Law Mean the End of Privacy?*, CHINAFILE (Apr. 22, 2015), https://www.chinafile.com/reporting-opinion/viewpoint/will-chinas-new-anti-terrorism-law-mean-end-privacy.

84. *See* Assemblée Nationale, Amendement No. 92CL (France) (introducing an amendment following the spate of 2015–2016 terrorist attacks in France).

85. *Id*.; Selyukh & Henn, *supra* note 82; Livingston, *supra* note 83.

86. *See infra* Sections V.F., V.G. (explaining that South Korea and the Netherlands have not weakened encryption and will use warrants to obtain data). As this comment does not have an exhaustive survey of countries, this analogy has the potential to be flawed.

87. *See infra* Sections V.H. (discussing the threat posed by ISIS members utilizing encryption technology).

Powers Bill in 2015.[88] British officials have explained the legislation's goals, arguing that encrypted messaging systems are acceptable under the new law provided that the companies can decrypt the messages when asked by the government.[89] The draft bill is not, therefore, an official ban on encryption but is functionally equivalent to a ban on end-to-end encryption. [90]

This draft bill resulted in a wave of lobbying from the tech industry. Apple and other tech giants (including Google and Microsoft) submitted a memorandum to a committee of Parliament which scrutinized the proposed law.[91] Apple has all but admitted that it will be placed in a position where it must comply with overlapping laws, but that it will "be left having to arbitrate between them, knowing that in doing so they might risk sanctions."[92] Companies have also warned the British government and the public that they will comply if they must, but costs to consumers will inevitably increase.[93] Matthew Hare, a chief executive of the Internet service provider Gigaclear, stated that "the indiscriminate collection of mass data is going to have a massive cost."[94]

In regards to the U.K. draft Investigatory Powers Bill, Wikipedia founder Jimmy Wales has stated, "[i]t is not possible in any sense of the word for the U.K. to ban encryption. More to the point, it's a moronic thing to do."[95] Accordingly, "[t]he problem noted by many last year is that a backdoor to encryption, even if euphemistically rebranded as a 'front door' or a 'golden key,' is by definition a vulnerability. Building in backdoors threatens consumers and makes them vulnerable to criminals and hostile foreign governments alike."[96] However, Wales has also stated that court-approved warrants would be a reasonable method to deal with Internet crime rather than backdoor access.[97] Golden keys, or secure encryption keys, have been called "mythical nonsense."[98]

Following the initial public and private response to the bill, it was revised to

88. Smith, *supra* note 67.

89. Matt Burgess, *Surveillance Bill Will Only Ban 'Strong' Encryption*, WIRED UK (Nov. 3, 2015), http://www.wired.co.uk/news/archive/2015-11/03/surveillance-bill-ban-strong-encryption-apple-imessage.

90. *Id*.

91. David Gilbert, *Apple Wades Into UK Encryption Debate Criticizing Investigatory Powers Bill*, INT'L BUS. TIMES (Dec. 21, 2015, 6:46 PM), http://www.ibtimes.com/apple-wades-uk-encryption-debate-criticizing-investigatory-powers-bill-2235532.

92. *Id*.

93. Alex Hern, *Broadband Bills Would Have to Increase to Pay for Snooper's Charter, MPs Are Warned*, GUARDIAN (Nov. 11, 2015, 7:55 AM), https://www.theguardian.com/technology/2015/nov/11/broadband-bills-increase-snoopers-charter-investigatory-powers-bill-mps-warned.

94. *Id*.

95. Kavita Iyer, *Wikipedia Founder Jimmy Wales Says Banning Data Encryption Is 'Moronic'*, TECHWORM (Oct. 9, 2015), http://www.techworm.net/2015/10/wikipedia-founder-jimmy-wales-says-banning-data-encryption-is-moronic.html.

96. *Id*.

97. *Id*. However, this seems to be inherently contradictory to Wales' own statements in the same article.

98. Jeong, *supra* note 48.

address some of the tech industry's concerns. Notably, the revised bill confirmed a power the government already retained, which was not part of the original draft. The British government already had the power to "covertly glean personal data for the purposes of 'preventing death or injury or damage to a person's physical or mental health.'"[99] This was seemingly extended in the revised draft bill by including language allowing access for investigation or prevention of a "serious crime."[100] Criticism from police chiefs that the bill provided too little power to police had an effect on the revisions as well, specifically in the type of web history that could be requested.[101] The bill originally only allowed police to identify the sender of a message "and where it was suspected an individual accessed illegal material. . . ."[102] After revision, the draft bill gave the power to ask for *any* web material that is "necessary and proportionate for a specific investigation."[103]

The draft bill, if passed, will likely create more disagreement, and possibly litigation, between the British government and the tech industry. A spokesperson of the Home Office, the governmental department in the U.K. responsible for immigration, counter-terrorism, police, drugs policy, and related science and research, was quoted saying that the government wants to "find a way to work with industry" that will ensure "that [the data of] terrorists and criminals [is accessible] in order to resolve police investigations and criminal acts."[104] Thus, the outcome of the bill will signify the U.K.'s position on encryption and the degree to which it values access over individual privacy concerns expressed by the tech industry.

B. People's Republic of China

The National People's Congress (NPC) of China recently developed an anti-terrorism law that would require companies to give encryption keys to public officials for any data that is stored on Chinese servers.[105] This would include data flows from domestic and international companies doing business in China.[106]

The law is a reaction to two recent developments. The first is the series of recent attacks carried out by terrorists centered in Xinjiang Uighur Autonomous Province;[107] and the second is the increased attention the Communist Party has been paying to the allegations of Edward Snowden regarding the U.S. government's surveillance programs.[108] The law has many provisions, the first two

99. Tom Whitehead, *Snoopers' Charter: Police Have Been Able to Hack into Phones and Computers for Routine Investigations for Years*, TELEGRAPH (Mar. 1, 2016, 2:00 PM), http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/12178483/Google-Apple-and-others-not-forced-to-break-in-to-encryption-unless-practicable-snoopers-bill-to-say.html.

100. *Id*.

101. *Id*.

102. *Id*.

103. *Id*.

104. Burgess, *supra* note 89.

105. Livingston, *supra* note 83.

106. *Id*.

107. *Id*.

108. *Id*.

of which are particularly relevant for discussion: (1) "[b]ackdoors must be made available to government authorities[,]"[109] and (2) "[e]ncryption [k]eys must be made available to government authorities."[110]

ChinaFile, the online magazine from the Center on U.S.-China Relations, stated that the law would have three major effects on global technology: 1) cyber-sovereignty might further alienate the Chinese Internet from the rest of the Internet; 2) Internet companies will see an increased opportunity to sell products within the Chinese market, but it will likely come at a higher cost; and 3) the international market for Chinese products will decrease.[111] Before the law passed, Scott Livingston, an American attorney specializing in Chinese trade and investment law, stated that "[c]ompanies with operations in China would be wise to familiarize themselves with the present draft, as its content and context may be instructive for understanding the future direction of China's Internet policy."[112]

Fu Ying, Spokesperson for the Chinese Parliament, stated that the laws will not affect tech companies' reasonable interests.[113] He also stated that many Western governments, including the U.S., have made similar demands.[114] Further, Fu stated that China's use of the encryption data will be more disciplined than American surveillance.[115] He hopes that "with transparent procedures, China's anti-terrorism campaign will be different from what the United States has done: letting the surveillance authorities run amok and turn counterterrorism into paranoid espionage and peeping on its civilians and allies."[116] This law was passed in December 2015, with its final version excluding some of the most controversial provisions.[117]

---

109. *Id*. Significantly, the draft of this law does not require that the government give notice when requesting a backdoor. *Id*.

110. Livingston, *supra* note 83. Articles 15 and 16 deal with this requirement, most relevant to this comment. Article 15 requires that Internet service providers "report their encryption scheme" to "departments responsible for encryption for examination" (likely the Office of State Commercial Cryptography Administration). *Id*. Article 16 "requires that ISPs that provide encrypted transmission services . . . file their encryption scheme with network communication departments and public security organs. . . ." *Id*. Article 16 also requires that ISP's subsequently help in any investigation that results from the inspection of an encryption scheme. *Id*.

111. *Id*.

112. *Id*.

113. Gerry Shih & Paul Carsten, *China Says Tech Firms Have Nothing to Fear from Anti-Terror Law*, REUTERS (Mar. 4, 2014, 4:14 AM), http://www.reuters.com/article/us-china-parliament-cybersecurity-idUSKBN0M00IU20150304.

114. *See id*. (indicating that Chinese telecom equipment manufacturers Huawei and ZTE Corp. have been effectively kept out of the U.S. market due to cybersecurity concerns).

115. Livingston, *supra* note 83.

116. *Id*.

117. *See* Shannon Tiezzi, *China's New Anti-Terrorism Law*, THE DIPLOMAT (Dec. 29, 2015), http://thediplomat.com/2015/12/chinas-new-anti-terrorism-law/ (stating that the statute provisions requiring companies to store user data on servers within China and to allow the Chinese government to review their encryption systems were replaced).

C. France

There has been movement towards regulating encryption in France, increasingly so following the Paris attacks in 2015.[118] The National Assembly, France's lower house of Parliament, has led the movement to regulate encryption.[119] A recent amendment to a penal reform bill added extensive punishments for smartphone manufacturers that do not comply with law enforcement requests.[120] The proposed law would require smartphone manufacturers to "provide access to data in connection with terrorism investigations."[121] If a company does not comply, there is a potential fine of up to $385,000.[122] In addition, executives of a non-complying company could face a potential five-year prison sentence.[123] This amendment (and the bill that it is attached to) would still need to pass the Sénat and be signed into law by the French President (currently President Hollande).[124]

D. India

India does not have an official law or response to the rise of encryption market-wide, but instead has waged individual battles with companies that employ the technology.[125] For example, a blanket law on encryption was passed in 2015 that requires individual citizens to keep the plaintext of any encrypted data they received for up to ninety days, and then to turn the plaintext over to security forces.[126] In response to public backlash, social media apps were exempted from the law.[127] In 2010, the Indian government nearly banned Blackberry for refusing to

---

118. *See* Don Reisinger, *French Law Would Fine Apple Over iPhone Encryption*, FORBES (Mar. 4, 2016, 12:52 PM), http://fortune.com/2016/03/04/french-law-apple-iphone-encryption/ (remarking on French politicians' efforts to address terrorism following the November 2015 Paris attacks).

119. *See id*. (discussing various proposals for reform with the National Assembly). Specifically, the push for penalizing smartphone makers has come from the right-wing opposition faction within the National Assembly. *Id*.

120. *Id*. There has been debate over the efficacy of this amendment in stopping the types of communications that it has been presumably drafted to stop. The amendment would punish smartphone manufacturers, but not the makers of widely-used applications that use encrypted technology (Facebook, Viber, etc.). Reisinger argues that providing a backdoor into hardware might grant some access (SMS messaging, Internet searches, etc.), but that applications could still be used to communicate, leaving law enforcement in the dark. *Id*. For the text of the amendment, see Assemblée Nationale, Amendement No. CL92 (France).

121. Reisinger, *supra* note 118.

122. *Id*.

123. *Id*.

124. *Id*.

125. *See, e.g.*, Ivan Mehta, *Indian Government Will Likely Not React Well to Whatsapp Turning on Encryption*, HUFFINGTON POST (June 4, 2016, 3:15 PM), http://www.huffingtonpost.in/2016/04/06/whatsapp-encryption_n_9621528.html.

126. *Id*.

127. *Id*.

give the government access to personal messaging systems.[128] There is much speculation over how the Indian government will handle the recent switch to end-to-end encryption by WhatsApp, a popular messaging system in India.[129]

E. Canada

Canada waged what at least one commentator has called a "quiet war on encryption."[130] While Canada has not yet spoken on the current end-to-end encryption debate, it is worthwhile to note the country's history with encryption. One significant way in which Canada has waged a "quiet war" on encryption is by widening the type of devices covered by its cryptography standards and weakening an important cryptographic standard.[131] Canadian mobile telecommunications providers must agree to and implement the Solicitor General's Enforcement Standards (SGES).[132] The standard relevant to this comment is standard twelve.[133] The annotation for the standard reads:

> Law enforcement requires that any type of encryption algorithm that is initiated by the service provider must be provided to the law enforcement agency unencrypted. This would include proprietary compression algorithms that are employed in the network. This does not include end to end encryption that can be employed without the service provider's knowledge.[134]

In 2012, the Canadian government expanded the scope of the SGES to include "circuit" forms of communication that were transmitted on new technologies.[135] SGES applies to mobile providers, but successive versions of "lawful access legislation" would theoretically apply to all telecommunications providers.[136] Bill C-13 was passed on December 9, 2014 and contains explicit clauses authorizing authorities to require telecommunications providers to decrypt certain communications.[137] Under Bill C-13, Canadian providers have the authority

---

128. *Id*. A deal was eventually struck between Blackberry and the Indian government that allowed the monitoring of Blackberry messaging and emails sent on the devices. *Id*.

129. *See id*. (discussing Indian encryption laws in the context of WhatsApp's switch to end-to-end encryption).

130. Christopher Parsons & Tamir Israel, *Canada's Quiet History of Weakening Communications Encryption*, UNIV. OF TORONTO: CITIZEN LAB (Aug. 11, 2015), https://citizenlab.org/2015/08/canadas-quiet-history-of-weakening-communications-encryption/.

131. *See id* (indicating that the Canadian government has cultivated an inadequate security standard such that Canadians are unable to communicate securely over voice or SMS messaging, unless using a third-party application).

132. *Id*.

133. "Standard twelve states, '[i]f network operators/service providers initiate encoding, compression or encryption of telecommunications traffic, law enforcement agencies require the network operators/service providers to provide intercepted communications en clair.'" *Id*. There are 22 standards. *Id*.

134. *Id*.

135. Parsons & Israel, *supra* note 130. Examples of circuit-based communications are SMS messaging, MMS messaging, fax, and voice-based communications. *Id*.

136. *Id.*

137. *Id*.

to challenge the demand.[138]

Canada's foreign signals intelligence agency, the Communications Security Establishment (CSE), has also played an active part in undermining global encryption mechanisms.[139] For example, the CSE ran a multi-national committee at the International Organization for Standardization.[140] This committee led to the NSA propagating and granting a sense of legitimacy to a method of encryption that is known to be vulnerable, the Dual EC DRBG.[141]

F. South Korea

The South Korean government has generally chosen to pursue individual surveillance and subsequent warrants to obtain user data.[142] A South Korean tech company, Daum Kakao, released a transparency report in January 2015 stating that the amount of warrants issued by the courts had quadrupled between 2012 and 2014.[143] Naver, a South Korean search portal, has seen the warrants issued for user data increase six times in the same period.[144] President Park Geun-Hye also recently announced increased surveillance for "any messages deemed as insulting to her or generally rumor-mongering."[145] This has pushed companies like Daum Kakao to change messaging systems by adding encrypted features.[146] It has also pushed users to use international messaging systems with encrypted features, like Telegram from Germany.[147]

G. The Netherlands

The Netherlands has taken a different approach than most countries in regard to legislation. In the "Government Position on Encryption," authored by the Minister of Security & Justice and the Minister of Economic Affairs, the Dutch

---

138. *Id*.

139. The CSE is Canada's primary cryptographic organization and its U.S. counterpart is the National Security Agency (NSA). The CSE has a history of intentionally "providing weak encryption to potential intelligence targets." *Id*.

140. *Id*.

141. Parsons & Israel, *supra* note 130. The Dual EC DRBG is the Dual Elliptic Curve Deterministic Random Bit Generator. Stephen Checkoway, et al., *On the Practical Exploitability of Dual EC in TLS Implementations*, DUAL EC 1, http://dualec.org/DualECTLS.pdf (last visited Oct. 26, 2016).

142. *See, e.g.*, Heewon Kim, *Korean Government Increases Warrants for Cyber Surveillance*, KOREA TIMES (Oct. 5, 2015), http://www.koreatimesus.com/korean-government-increases-warrants-for-cyber-surveillance/; Russell Brandom, *Surveillance Drives South Koreans to Encrypted Messaging Apps*, VERGE (Oct. 6, 2014, 5:27 PM), http://www.theverge.com/2014/10/6/6926205/surveillance-drives-south-koreans-to-encrypted-messaging-apps.

143. Kim, *supra* note 142.

144. *See* Kim, *supra* note 142 (stating warrants for user information increased from 1487 in 2012 to 9342 in 2014). For more information about Naver, see generally *Company Overview*, NAVER, https://www.navercorp.com/en/company/companyInfo.nhn (last visited Oct. 20, 2016).

145. Brandom, *supra* note 142.

146. Kim, *supra* note 142.

147. Brandom, *supra* note 142.

declared that a strongly encrypted Internet was in the country's best interest.[148] Therefore, the Dutch government will not be mandating encryption backdoors of any kind.[149] The Ministers said "[i]t is currently not desirable to take restricting legal measures concerning the development, availability, and use of encryption within the Netherlands."[150] Also noteworthy was the statement by the Dutch government that backdoors would create "undesirable consequences for the security of communicated and stored information" because "digital systems can become vulnerable to criminals, terrorists and foreign intelligence services."[151]

H. ISIS

ISIS is known to use the encrypted app Telegram from Germany to communicate amongst its adherents, spread propaganda, and recruit new followers.[152] The terror group continues to use the app even after Telegram took action to shut down several of its channels following the Paris attacks in 2015.[153] Telegram co-founder, Pavel Durov, is a noted privacy rights advocate.[154] Durov relented to government pressure following the Paris attacks and shut down seventy-eight messaging channels used by ISIS.[155]

VI. THE AMERICAN BATTLE OVER ENCRYPTION

The battle over encryption has grown significantly both internationally and domestically in the U.S. in recent years. The U.S. reached a watershed moment in the controversy between Apple and the FBI, when Apple's refusal to comply with the court order of Federal Magistrate Judge Sheri Pym to help decrypt the phone of one of the San Bernardino shooters set off a firestorm of criticism,[156] but also

148. Matthijs R. Koot, *Full Translation of the Dutch Government's Statement on Encryption*, MATTHIJS R. KOOT'S NOTEBOOK (Jan. 5, 2016), https://blog.cyberwar.nl/2016/01/full-translation-of-the-dutch-governments-statement-on-encryption/.

149. *Id*.

150. *Id*.

151. Glyn Moody, *Dutch Government: Encryption Good, Backdoors Bad*, ARS TECHNICA (Jan. 6, 2016, 11:21 AM), http://arstechnica.com/tech-policy/2016/01/dutch-government-encryption-good-backdoors-bad/ (quoting Koot, *supra* note 148).

152. *See* Pamela Engel, *ISIS Has Figured Out Ways to Get Around Restrictions on One of the Main Apps It Uses for Propaganda*, BUS. INSIDER (Nov. 24, 2015, 4:46 PM), http://www.businessinsider.com/isis-telegram-channels-2015-11 (describing the finding by Telegram of channel feature used by ISIS to circulate unlimited number of messages to thousands of followers).

153. *Id*.

154. Sara Ashley O'Brien, *Who Is Telegram Founder Pavel Durov?*, CNN MONEY (Dec. 17, 2015, 5:27 PM), http://money.cnn.com/2015/12/17/technology/telegram-pavel-durov/.

155. Parmy Olson, *Messaging App Telegram Shuts Down 78 ISIS Propaganda Channels*, FORBES (Nov. 19, 2015, 7:49 AM), http://www.forbes.com/sites/parmyolson/2015/11/19/telegram-isis-propaganda-channels/#16fc639d6f88.

156. Asif, *supra* note 1. Opposing Apple's refusal to comply with the government's request, Donald Trump argued that consumers should boycott the company's products until it agreed to assist the authorities in their investigation. Similarly, the Department of Justice accused Apple of refusing simply as a means of receiving public exposure. *Id*.

garnered public support from other tech giants such as Google, Microsoft, Facebook, Twitter and Huawei.[157]

Per a Government Status Report filed March 28, 2016 in federal court, the FBI gained entry into the San Bernardino shooter's iPhone without the assistance of Apple, and the case is now closed.[158] However, future U.S. regulatory steps will greatly impact the debate over the role of encryption in American society. This comment argues that the U.S. should defer to the expertise of the tech industry on the dangers of regulating encryption. Allowing back-door access for law enforcement or national security agencies makes systems vulnerable to attacks by hackers and hostile nations. Making U.S. systems more secure while other countries make theirs vulnerable allows the U.S. to be comparatively safer.

A. The United States' Regulatory Options

It seems unlikely that any new legislation overhauling cyber-privacy will do so to the same degree as recent British or Chinese legislation.[159] This can be attributed to several factors. First, domestic political pressures regarding surveillance and privacy are at a boiling point following the Edward Snowden revelations of 2013.[160] Second, requiring access to all encrypted communications through any technological medium would likely stymie innovation in the global tech industry.[161] Third, new overhauling legislation would also increase tension between different markets purchasing products from these companies, as almost any scheme chosen by the U.S. would likely have a vast precedential effect across the globe.

The dispute between Apple and the FBI points to the likelihood that the U.S. is moving towards creating regulations that provide for more access, but limited to special emergency situations such as terrorist attacks. If the U.S. decides not to regulate, that could lend official legitimacy to the position of the tech industry that

---

157. Ellen Nakashima, *Apple Vows to Resist FBI Demand to Crack iPhone Linked to San Bernardino Attacks*, WASH. POST (Feb. 17, 2016), https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html; *see also* Asif, *supra* note 1 (listing prominent tech companies that stood behind Apple in its refusal to provide a backdoor to the government partly due to the fear of the precedent this case will set.).

158. Selyukh, *supra* note 4.

159. Investigatory Powers Bill 2015–16, HC Bill [143] (U.K.).

160. *See NSA Leaks: A Timeline*, AL JAZEERA AMERICA, http://america.aljazeera.com/watch/shows/fault-lines/FaultLinesBlog/2013/11/1/nsa-leaks-a-timeline.html (last visited Oct. 21, 2016) (citing various headlines since Snowden's leak concerning NSA surveillance and data privacy). Snowden was responsible for leaking classified National Security Agency (NSA) documents to the public. For example, the NSA's spying capabilities pertaining to each country were revealed, as well as the fact that the agency had collected nearly 3 billion pieces of intelligence on U.S. citizens. *Id*.

161. *See* Paul Mozur, *New Rules in China Upset Western Tech Companies*, N.Y. TIMES (Jan. 28, 2015), http://www.nytimes.com/2015/01/29/technology/in-china-new-cybersecurity-rules-perturb-western-tech-companies.html (indicating that the proposed antiterrorism law could present a new barrier for tech companies seeking to access the Chinese market).

strong security systems are essential. If the U.S. were to embrace the previously discussed PrivaTegrity scheme created by David Chaum, that could have far-reaching implications, as well. In examining how the U.S. should best address the regulation of encryption in the future, it is necessary to look at how the U.S. has addressed encryption prior to the current dispute between Apple and the FBI.

B. Historical Context

American statutes regarding encryption have often centered around the ability of international criminal and terrorist groups to encrypt data and use that data to hurt the U.S.' national security and economic interests.[162] Since the 1990s, there have been various regulations on the export of encryption software.[163] Until 1996, this was done by classifying encryption software as "munitions."[164] Classifying encryption software as such brought it within the purview of the State Department, and was looked at as a "defense article."[165] The export of encryption, however, is governed by the Arms Export Control Act (AECA) and the Export Administration Act (EAA). The AECA is administered by the State Department under the International Traffic in Arms Regulations (ITAR), and the EAA is administered by the Commerce Department under the Export Administration Regulations.[166] A licensing system, with limited exceptions, primarily enforces these regulations.[167]

American regulation of encryption exports has been challenged multiple times in U.S. courts. In *Bernstein v. United States Department of State*, the petitioner, Daniel Bernstein, sought to publish the source code of encryption software that he had written on the Internet, but he was denied a license by the State Department.[168] Bernstein challenged the application of the AECA and ITAR to the publication of encryption source code, arguing that the denial of a license was a form of prior restraint.[169] Ruling in favor of Bernstein, the court held that source code is speech, which had the effect of loosening export regulations for encryption software.[170] In *Karn v. United States Department of State*, a book of encryption algorithms was ruled also to be speech, but a diskette containing identical information was ruled

162. *See* Saunders, *supra* note 15 ("The growing use of encryption has led to concerns on the part of federal law enforcement and national security authorities that these technologies will be employed for criminal and terrorist purposes.").

163. *Id*.

164. *Id*. at 950.

165. *See The International Traffic in Arms Regulations (ITAR)*, U.S. DEP'T OF ST., https://www.pmddtc.state.gov/regulations_laws/itar.html (last visited Oct. 20, 2016) (indicating that the U.S. Munitions List is regulated by the Department of State).

166. Saunders, *supra* note 15, at 949–950.

167. *Id*.

168. Bernstein v. U.S. Dep't of St., 922 F. Supp. 1426 (N.D. Cal. 1996).

169. *Id*. The United States District Court for the Northern District of California, as well as the United States Court of Appeals for the Ninth Circuit, ruled that the petitioner was engaging in "speech" by publishing their source code, and that the regulation therefore violated the First Amendment. *Id*.

170. Saunders, *supra* note 15, at 951–952.

not to be speech.[171] The diskette instead was ruled to be cryptographic software, and the court ruled that judicial review of the President's designation of an item as a defense article is barred by AECA § 2778.[172] *Karn* is significant because the District of Columbia (DC) District Court held that AECA and ITAR are constitutional because they furthered an important or substantial government interest.[173] The *Karn* court also held that ITAR does not constitute a prior restraint on free speech, because the regulations are content-neutral.[174]

In 1993, the White House introduced the "Clipper Chip Initiative" as an effort to regulate encryption.[175] The Clipper Chip would have subjected electronic encryption technology to key escrow in order for the government to hold a key to decode messages.[176] Key escrow keeps a record of the key for each device with a Clipper Chip installed.[177] Before two devices with Clipper Chip would communicate, the chips would create a string of data called the "Law Enforcement Access Field" ("LEAF").[178] The LEAF would provide the government with the digital signature necessary to obtain the keys and decrypt the communication.[179]

The Clipper Chip initiative, however, failed due to what has been called "a firestorm of protest on constitutional and economic grounds."[180] The successful hacking of the Clipper Chip by Matt Blaze also contributed to the Clipper Chip not being adopted by the tech industry.[181] Battles between law enforcement and the tech industry over the Clipper Chip have colloquially been referred to as "The Crypto Wars."[182]

---

171. Karn v. U.S. Dep't of St., 925 F. Supp. 1 (D.D.C. 1996).

172. *Id*. at 6.

173. Saunders, *supra* note 15, at 952.

174. *Id*.

175. Press Release, Office of the Press Secretary, White House Announcement of Clipper Initiative (Apr. 16, 1993).

176. A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 715–16 (1995).

177. Sean Gallagher, *What the Government Should've Learned about Backdoors from the Clipper Chip*, ARS TECHNICA (Dec. 14, 2015, 4:05 PM), http://arstechnica.com/information-technology/2015/12/what-the-government-shouldve-learned-about-backdoors-from-the-clipper-chip/.

178. *Id*.

179. *Id*.

180. Saunders, *supra* note 15, at 952.

181. Blaze is a cryptology researcher (amongst other topics) and currently an Associate Professor of Computer and Information Science at the University of Pennsylvania. Matt Blaze, *Research Summary and Bio*, CRYPTO.COM, http://www.crypto.com/research.html (last visited Oct. 21, 2016). For a personal account of Mr. Blaze's hacking of the Clipper Chip, see Matt Blaze, *Looking Back at the Clipper* Chip, CRYPTO.COM, http://www.crypto.com/papers/escrow-acsac11.pdf (last visited Oct. 26, 2016). For the paper that Mr. Blaze wrote breaking the story of the hacking, see Matt Blaze, *Protocol Failure in Escrowed Encryption Standard*, CRYPTO.COM, http://www.crypto.com/papers/eesproto.pdf (last visited Oct. 26, 2016).

182. Greenberg, *supra* note 44.

C. The Current Battle over Encryption

In January of 2015, President Barack Obama stated "if we find evidence of a terrorist plot . . . and despite having a phone number, despite having a social media address or email address, we can't penetrate that, that's a problem."[183] Calling tech companies "patriots," President Obama said in the same statement that he believes they would like to help solve the problem.[184] These statements were made after meetings with then U.K. Prime Minister David Cameron, with Cameron at Obama's side.

In September of 2015, however, a leaked memorandum from the National Security Council (NSC) contradicted the President's earlier stance.[185] This memorandum was mostly devoid of technical substance and instead posed political solutions.[186] The Administration saw itself with three political options in handling the fight over end-to-end encryption.[187] The first would be to plainly oppose new laws and new backdoors and to speak favorably about encryption.[188] The second would be to defer the issue and consult with experts.[189] The third option would be to "punt the issue into the long grass."[190] In a surprising turn, however, the memorandum pushes the first option the most.[191] "Overall, the benefits to privacy, civil liberties, and cybersecurity gained from encryption outweigh the broader risks that would have been created by weakening encryption."[192] The memorandum's position seems to indicate that there are possibly different factions of the Executive Branch of the U.S. government that have diverging stances on encryption.

In October 2015, the Obama Administration stated that they will not attempt to pass new laws regulating end-to-end encryption.[193] In a written statement to the Senate Homeland Security and Governmental Affairs Committee, FBI Director James Comey stated "the administration has decided not to seek a legislative remedy now but that it makes sense to continue the conversations we are having

---

183. Danny Yadron, *Obama Sides with Cameron in Encryption Fight*, WSJ BLOG (Jan. 16, 2015, 4:52 PM), http://blogs.wsj.com/digits/2015/01/16/obama-sides-with-cameron-in-encryption-fight/.

184. *Id*.

185. Kieren McCarthy, *Obama Edges towards Full Encryption - but Does He Understand What That Means?*, REGISTER (Sept. 16, 2015, 10:46 PM), http://www.theregister.co.uk/2015/09/16/obama_edging_toward_support_for_encryption/.

186. *See* Nat'l Sec. Council, Review of Strategic Approaches (leaked manuscript), https://assets.documentcloud.org/documents/2426450/read-the-nsc-draft-options-paper-on-strategic.pdf (discussing policy strategies regarding encryption without technical details).

187. McCarthy, *supra* note 185.

188. *Id*.

189. *Id*.

190. *Id*.

191. *Id*.

192. *Id*.

193. Ellen Nakashima & Andrea Peterson, *Obama Administration Opts Not to Force Firms to Decrypt Data-For Now*, WASH. POST (Oct. 8, 2015), 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.

that are very productive."[194] There is speculation that perhaps the Obama Administration will change course in 2016 following the terrorist attacks in Paris and San Bernardino.[195] Members of the Obama Administration, as well as congressional allies of the Administration, have been increasingly critical of encrypted messaging following the Paris attacks.[196]

1. Legislative Branch Positions

The House Judiciary and the House Energy and Commerce Committee have set up a bipartisan working group to "examine the complicated legal and policy issues surrounding encryption."[197] The group has been tasked with identifying "potential solutions that preserve the benefits of strong encryption – including the protection of American[] benefits of strong encryption – while also ensuring law enforcement has the tools needed to keep us safe and prevent crime."[198] The group, according to its own press release, has jurisdiction over the entire nexus between these issues.[199]

Senator Richard Burr (R-N.C.) and Senator Dianne Feinstein (D-Calif.), the chairman and vice chairwoman of the Senate Intelligence Committee, introduced legislation on April 13, 2016 that "mandate[s] that companies assist law enforcement in accessing content shielded by encryption."[200] There is also draft legislation to form a commission to examine the effect of encryption on national security. Rep. Michael McCaul (R-Tex.), the chairman of the House of Representatives Homeland Security Committee, and Senate Intelligence Committee member Mark Warner (D-Va.) have drafted legislation to establish the commission.[201] McCaul plans for the commission to be comprised of "technologist[s], privacy activists, academics, and law enforcement official[s]."[202]Also planning to have input in the commission is Representative Will Hurd (R-Tex.), who worked prior to his congressional career for a cybersecurity

194. *Id*.

195. Russell Brandom, *How San Bernadino Changes the FBI's War on Encryption*, VERGE (Mar. 29, 2016, 11:31 AM), http://www.theverge.com/2016/3/29/11325030/apple-fbi-iphone-hack-security-encryption-what-comes-next.

196. Alina Selyukh, *After Paris Attacks, Encrypted Communication Is Back in Spotlight*, NPR (Nov. 16, 2015, 11:30 PM), http://www.npr.org/sections/alltechconsidered/2015/11/16/456219061/after-paris-attacks-encrypted-communication-is-back-in-spotlight.

197. Press Release, House of Representatives Judiciary Committee, Goodlatte, Conyers, Upton, and Pallone Announce Bipartisan Encryption Working Group (Mar. 21, 2016), https://judiciary.house.gov/press-release/goodlatte-conyers-upton-pallone-announce-bipartisan-encryption-working-group/.

198. *Id*.

199. *Id*.

200. Amir Nasr, *A Tale of Two Encryption Bills*, MORNING CONSULT (Mar. 23, 2016), https://morningconsult.com/2016/03/a-tale-of-two-encryption-bills/.

201. *Id*.

202. Sean Lyngaas, *McCaul Advisor Sees Digital Security Commission Launching Soon*, FCW (Jan. 14, 2016), https://fcw.com/articles/2016/01/14/encryption-commission-lyngaas.aspx.

firm.[203] This legislation is considered more likely to become law than the Feinstein-Burr proposal, possibly because it is more moderate in its approach.[204]

Senator Chuck Grassley (R-Iowa), the chairman of the Senate Judiciary Committee, has also sent a letter to Deputy Attorney General Sally Yates in which he voiced support for Comey's positions:[205] "Countries like Great Britain and France are much further along in their national dialogues about how best to balance privacy and public safety with regard to encryption and are currently contemplating specific legislative proposals to address the threat posed by widespread inviolable encryption."[206]

Following the Paris attacks, Senator John McCain (R-Ariz.) publicly expressed support for legislating encryption.[207] Senator McCain stated: "In the Senate Armed Services we're going to have hearings on it and we're going to have legislation."[208] He also stated that the non-legislative status quo is "unacceptable."[209] Former Representative Mike Rogers (R-Mich.), once the chairman of the House Permanent Select Committee on Intelligence, also recently publicly criticized moves towards end-to-end encryption.[210] In an op-ed for CNN's website, Rogers states that encryption technology poses a significant security risk to the U.S.[211] Rogers argues it does this by allowing radicalized individuals to communicate in a manner that is not accessible either by law enforcement or by the companies that are facilitating the communication.[212] Rogers posits that the American tech industry has made sacrifices to its bottom line before in the name of the public good, and the tech industry acquiescing on end-to-end encryption would keep the public safe.[213]

2. U.S. Law Enforcement Positions

The majority of domestic anti-encryption rhetoric comes from U.S. law enforcement institutions. The most vocal opponent of end-to-end encryption is

---

203. *Id*.

204. *See* Nasr, *supra* note 200 (discussing the likelihood of either the Feinstein-Burr or the McCaul-Warner bills becoming law).

205. Sean Lyngaas, *Grassley Tries to Revive 'Going Dark' Legislative Fix*, FCW (Oct. 9, 2015), https://fcw.com/articles/2015/10/09/grassley-encryption-going-dark.aspx.

206. *Id*.

207. Chris Smith, *McCain Wants to Legislate Encryption Even Though There's No Evidence It Helped ISIS in Paris Attacks*, BGR (Nov. 19, 2015, 9:26 AM), http://bgr.com/2015/11/19/paris-attacks-encryption-debate/.

208. *Id*.

209. *Id*.

210. Rogers is also a Westwood One Radio Host, a CNN commentator on national security, and advises technology and cybersecurity companies. Mike Rogers, *Encryption a Growing Threat to Security*, CNN (Aug. 1, 2015, 7:57 AM), http://www.cnn.com/2015/08/01/opinions/rogers-encryption-security-risk/.

211. *Id*.

212. *Id*.

213. *See id*. (indicating that tech companies can balance their bottom line with public safety).

James Comey, Director of the FBI.[214] Director Comey argues that end-to-end encryption forces the FBI to "go dark" on investigations.[215] Director Comey has stated that there are "societal costs to universal encryption,"[216] and that if law enforcement cannot access information and save lives, the nation would be in a "very dark place."[217] Director Comey's solution would create a specific passcode or key to decode encrypted messages that would only be available to law enforcement.[218]

William Bratton, the former Commissioner of the New York City Police Department (NYPD) also critiqued end-to-end encryption and encrypted communications in general, arguing that encrypted communications have made it "impossible for officials to collect warnings on terrorist attacks."[219] Commissioner Bratton takes his critique one step further, effectively alleging that tech companies profit from the commercialization of secrecy: "We, in many respects, have gone blind as a result of the commercialization and the selling of these devices, that cannot be accessed either by the manufacturer or, more importantly, by us in law enforcement, even equipped with search warrants and judicial authority."[220]

The National Security Agency (NSA) and its parent agency, the Department of Defense (DOD), have released conflicting statements regarding encryption.[221] Statements from the CIA further muddle a coherent stance on encryption.[222] The

---

214. *See FBI Executives*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/about-us/executives/comey (last visited Oct. 24, 2016) (containing the biography of James Comey).

215. Lorenzo Franceschi-Bicchierai, *Encryption Is 'Depressing,' the FBI Says*, MOTHERBOARD (May 21, 2015, 12:37 PM), http://motherboard.vice.com/read/encryption-is-depressing-the-fbi-says. "Going dark" refers to not being able to access key information during an investigation. *Id*.

216. *Id*.

217. *Id.*

218. *Id*.

219. *See* J. David Goodman, *New York City Police Commissioner Says Attacks Will Force Changes in Tactics*, N.Y. TIMES (Nov. 16, 2015, 1:38 PM), http://www.nytimes.com/live/paris-attacks-live-updates/bratton-says-attacks-will-force-law-enforcement-to-change-tactics ("This is something that is going to need to be debated very quickly because we cannot continue operating where we are blind in the area of gathering intelligence on potential attacks"); *see also* Sanger & Perlroth, *supra* note 50 (noting Bratton's assertion that officials are blinded by encryption).

220. Sanger & Perlroth, *supra* note 50.

221. *See* Tim Cushing, *Dept. of Defense Defends Strong Encryption While Its Impetuous Child-The NSA-Continues to Lament the Coming Darkness*, TECHDIRT (July 6, 2015, 8:38 AM), https://www.techdirt.com/articles/20150703/14441931535/dept-defense-defends-strong-encryption-while-impetuous-child-nsa-continues-to-lament-coming-darkness.shtml (highlighting that while FBI and NSA see encryption as leaving agencies in the dark, the DOD prefers stricter encryption); *see also* Kevin Collier, *The NSA Is Renting Its Technology to U.S. Companies*, DAILY DOT (Dec. 11, 2015, 6:58 PM), http://www.dailydot.com/layer8/nsa-technology-transfer-program-national-security-agency-ttp/ (indicating that the NSA falls under the umbrella of the DOD).

222. *See* Selyukh, *supra* note 196 (indicating how CIA Director Brennan viewed the Paris attacks as a "wake-up call" to the need to reform encryption policy); *see also infra* note 219 and accompanying text (indicating that the Paris attacks should be seen as a wake-up call for encryption reform).

NSA's statements are similar to statements made by the FBI, voicing concerns about "going dark" and how that will affect the agency's ability to properly fulfill its mission.[223] NSA Director Admiral Michael S. Rogers has suggested requiring companies to create a digital key for certain devices but dividing the key into pieces so that interpersonal or interagency cooperation would be needed to use it.[224]

Officials from the DOD, however, have recently supported end-to-end encryption.[225] In an interview, security expert and former Vice Chairman of the Joint Chiefs of Staff Admiral James A. Winnefeld responded to a question by stating: "[B]ut I think we all win if our networks are more secure. And I think I would rather live on the side of secure networks and a harder problem for Mike on the intelligence side [speaking of Adm. Michael S. Rogers of the NSA] than very vulnerable networks and an easy problem for Mike."[226]

In a speech on encryption on November 16, 2015 at the Center for Strategic and International Studies, CIA Director John Brennan provided statements which seemed to put the CIA's relative views on privacy and national security into perspective, hoping that the recent Paris attacks would be a "wake-up call."[227] Former CIA Deputy Director Michael Morell has also stated that, at the very least, the Paris attacks will renew the American discussion over end-to-end encryption. [228]

VII. THE U.S. SHOULD DEFER FROM CRAFTING NEW ENCRYPTION REGULATIONS

The global debate over end-to-end encryption is complex and hard to navigate. One of the primary reasons that it is difficult to form any sort of nuanced understanding or coherent policy proposal is because there are so many different

223. *See* Nakashima & Gellman, *supra* note 57 (noting that requiring the agency to use "brute-force" methods is time-consuming and that obtaining covert access to manufacturers requires an often unavailable level of specialty).

224. *Id*.

225. Cushing, *supra* note 221.

226. *Id*.

227. See Selyukh, *supra* note 196 (indicating the Paris attacks would be a wake-up call for increasing ways to deal with encryption). Brennan stated: "There has been a significant increase in the operational security of a number of these operatives and terrorist networks as they've gone to school on what it is that they need to do in order to keep their activities concealed from the authorities. And as I mentioned, there are a lot of technological capabilities that are available right now that make it exceptionally difficult both technically as well as legally for intelligence security services to have the insight they need to uncover it." *Brennan Delivers Remarks at the Center for Strategic & International Studies Global Security Forum 2015,* Central Illigence Agency (Nov. 16, 2015), https://www.cia.gov/news-information/speeches-testimony/2015-speeches-testimony/brennan-remarks-at-csis-global-security-forum-2015.html.

Brennan continued: "In the past few years because of a number of unauthorized disclosures and a lot of hand-wringing over the government's role in the effort to try to uncover these terrorists, there have been some policy and legal and other actions that are taken that make our ability, collectively, internationally, to find these terrorists much more challenging. And I do hope that this is going to be a wake-up call." *Id*.

228. Alexander Howard, *After Paris, What We're Getting Wrong in 'Privacy vs. Security' Debate*, HUFFINGTON POST (Nov. 16, 2015, 3:14 PM), http://www.huffingtonpost.com/entry/paris-attacks-privacy-vs-security_us_5649d222e4b045bf3defcd0e.

requirements amongst varied nations.[229] The varied standards are a problem because, according to tech experts, any amount of access can make a system more vulnerable.[230] However, this comment argues that the U.S. should hold off on crafting new regulations, as being patient throughout the duration of this debate will make the U.S. comparatively safer than other nations. Full encryption makes us safer, and while other countries are making their own systems more vulnerable, we should be strengthening our communication systems instead.

Smartphone data has undoubtedly been helpful in obtaining information and capturing criminals. [231] According to François Molins, the Chief Prosecutor of Paris, smartphone data was critical in investigating those responsible for the attacks on Charlie Hebdo magazine on January 7, 2015.[232] Molins also has stated that it was integral into the investigation of an attack on a gas station in Saint-Quentin-Fallavier in June of 2015.[233]

As authors of a recent op-ed in The New York Times argued, in at least seventy-four legal proceedings in Manhattan between October of 2013 and June of 2014, iPhones were inaccessible because of the phones' encryption.[234] The iPhones were connected to investigations of child sexual abuse, sex trafficking, and many other violent crimes.[235] Following the recent court order served upon Apple by Judge Pym,[236] Cyrus Vance, Jr., District Attorney of Manhattan, stated that he has 175 phones currently waiting to be unlocked.[237] Access to these phones could allow law enforcement to prosecute the perpetrators of these crimes and prevent further criminal acts.

The benefits of end-to-end encryption, however, outweigh the possible security drawbacks. A completely secure network is more secure than a partially secure network, even if the part that is unsecure is small. It is better to fight crime with the tools we have than to open the floodgates. *The Intercept*, an online journal seeking to hold governments and corporations accountable,[238] has claimed that many of the statistics and anecdotes used by law enforcement to justify advocating

---

229. *See generally* Nathan Saper, *International Cryptography Regulation and the Global Information Economy*, 11 NW. J. TECH. & INTELL. PROP. 673 (2013).

230. *See*, *e.g.*, Jeong, *supra* note 48.

231. *See* Vance et al., *supra* note 51 (discussing recent shootings and smartphone security).

232. *Id*.

233. *Id*.

234. *Id*.

235. *Id*.

236. *See generally* Eric Lightblau, *Judge Tells Apple to Help Unlock iPhone Used by San Bernardino Gunman*, N.Y. TIMES (Feb. 16, 2016), http://www.nytimes.com/2016/02/17/us/judge-tells-apple-to-help-unlock-san-bernardino-gunmans-iphone.html.

237. Alyssa Newcomb, *New York DA Says He Can't Access 175 iPhones from Criminal Cases Due to Encryption*, ABC NEWS (Feb. 18, 2016 1:34 PM), http://abcnews.go.com/Technology/york-da-access-175-iphones-criminal-cases-due/story?id=37029693.

238. *About & Contacts*, THE INTERCEPT, https://theintercept.com/staff/ (last visited Oct. 25, 2016).

for stronger encryption controls are not factually correct.[239] Citing a Federal Courts report on wiretapping, *The Intercept* stated that in only four cases were state and federal police obstructed by encryption.[240] In a direct investigation into the claims made by FBI Director Comey, *The Intercept* found that Comey had actually misconstrued several stories that he told in speeches supporting encryption controls.[241]

Providing access to encrypted data for law enforcement agencies and other governmental bodies across the world makes all related encrypted systems more vulnerable, which in turn makes the global population more susceptible to cyber-attacks and hacking.[242] The previously mentioned *Keys Under Doormats* report thoroughly explains the technical risks associated with governments weakening encryption in the name of law enforcement.[243] The report lists three reasons why regulating encryption results in systems is less safe than what exists currently.[244] The first is that providing exceptional access to these communications would force tech companies to make a "U-turn from the best practices now being deployed to make the Internet more secure."[245] Tech companies have been increasingly utilizing "forward secrecy," which requires that transaction keys are discarded after every transaction in which they are used.[246] Forward secrecy means that hackers have less to work with, and historical data is safe.[247] Requiring exceptional access would make data more vulnerable because if the access key was hacked, there would be much more information for the potential hacker to recover.[248] Allowing more information to be vulnerable to a hack is certainly an important risk to consider.

The second concern expressed in *Keys Under Doormats* is that access would increase complexity, and therefore increase vulnerability.[249] The report begins this analysis with the premise that if "exceptional access" (government access to encrypted information) were to be applied throughout the industry, it would create "widespread exceptional access," meaning use beyond the government.[250] While

239. *See* McLaughlin, *supra* note 53 (claiming that the examples the FBI relied upon to justify weakening encryption had nothing to do with encryption).

240. *Id*.

241. *See* Dan Froomkin & Natasha Vargas-Cooper, *The FBI Director's Evidence Against Encryption is Pathetic*, INTERCEPT (Oct. 17, 2014, 12:49 PM), https://theintercept.com/2014/10/17/draft-two-cases-cited-fbi-dude-dumb-dumb/ (finding that encryption had not been a barrier to identifying or capturing culprits, despite Comey's assertion that encryption could lead law enforcement to miss crucial evidence).

242. *See* Jeong, *supra* note 48 (noting that building any backdoors threatens consumers); *see also* Cushing, *supra* note 221 (noting that DOD supports end-to-end encryption).

243. *See* Abelson et al., *supra* note 6, at 15 (stating that the *Keys Under Doormats* report was a comprehensive report on end-to-end encryption and the risks of government access released in 2015 by MIT).

244. *Id*. at 2.

245. *Id*.

246. *Id*. at 12.

247. *Id*.

248. *Id*.

249. Abelson et al., *supra* note 6, at 2.

250. *Id*.

this is not the position this comment takes, the consequences the report lists are still important to consider. To achieve access, new technologies would need to be deployed and tested, which would increase a system's vulnerabilities.[251] As Dr. Frederick R. Chang, the former head of research for the NSA, testified before the U.S. Congress in 2013, "[i]ndeed it has been said that complexity is the enemy of security."[252] To allow our encryption systems to become exponentially more complex is to allow for an increase in vulnerabilities. This is an unacceptable risk.

The final risk discussed by *Keys Under Doormats* is that allowing exceptional access for law enforcement will put a focus on who bad actors should aim to attack.[253] The report cites the hacking of the Office of Personnel Management (OPM) of 2015 as an example of "how much harm can arise when many organizations rely on a single institution that itself has security vulnerabilities."[254] This is the risk given by the report that is the most persuasive. To allow for exceptional access is to trust our most complex technological systems to the hands and minds of those that are not the most technologically capable.

Bruce Schneier, a board member of the Electronic Frontier Foundation (EFF) and noted tech commentator,[255] has stated that many of the most noted tech security failures of recent history are correlated to failures in encryption technology.[256] These failures are evidenced in such instances as the Chinese government's hack of the OPM and the hacks of the TJX Companies and Target Corporation.[257] Clearly, a hack akin to the OPM hack affects our national security, as the names and personal information of government workers are involved. However, private corporations that are hacked can also affect our national security. These hacks could be training for later attacks on federal or other government entities. Also, federal employees and agencies are likely regular customers with these types of

---

251. *Id*.

252. *Id*. at 16.

253. *Id*. at 2.

254. *See id*. (explaining that the attack on the OPM caused multiple federal agencies to lose important data because they used a single organization, OPM, which had an infrastructure security breach); *see also* Ellen Nakashima, *Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say*, WASH. POST (July 9, 2015), https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/ ("Two major breaches last year of U.S. government databases holding personnel records and security-clearance files exposed sensitive information about at least 22.1 million people, including not only federal employees and contractors but their families and friends.").

255. Schneier is also a fellow at Harvard's Berkman Institute, the Chief Technology Officer of Resilient Systems, and is regularly published for his commentary on security issues. *See, e.g.*, Bruce Schneier, *About Me*, SCHNEIER.COM, https://www.schneier.com/ (last visited Oct. 26, 2016).

256. Bruce Schneier, *How an Overreaction to Terrorism Can Hurt Cybersecurity*, MIT TECH. REV. (Jan. 25, 2016), https://www.technologyreview.com/s/545716/how-an-overreaction-to-terrorism-can-hurt-cybersecurity/.

257. *Id*.

companies, and any type of information could be found and exploited in a hack.[258] With stronger encryption, or at least less vulnerable networks, these hacks would likely be much more difficult. As Nuala O'Connor stated, "the sophistication and number of cyber attacks on the security of individuals, businesses, government agencies, and critical infrastructure are only increasing."[259]

Apple v. FBI also highlighted a third concern stated in *Keys Under Doormats*—that to concentrate focus on a specific set of actors is to introduce an unacceptable risk due to the possibility that one of those actors could be compromised.[260] Focusing on a specific set of actors would draw attention and create an enlarged risk due to exceptional access; a third party, such as law enforcement, would have security access to all actors of interest.[261] If one of the parties of interest was attacked, there is an increased potential that the attacker would be able to access other associated actors' information since they could access the keys to all associated actors through a third party.[262]

There is also an argument that "going dark" is the wrong metaphor, and that encryption does not significantly hinder law enforcement's legitimate investigative tactics. The authors of a report called *Don't Panic: Making Progress on the "Going Dark" Debate*, published by the Berkman Center for Internet & Society at Harvard University, recently argued this point.[263] The authors of *Don't Panic* state that due to several factors,[264] the gaps in information left by encryption will be filled.[265] This is outside the scope of this comment, but it is worth noting that according to this paper's thesis, encryption does not make us less safe, and

---

258. *See* Abelson et al., *supra* note 6, at 2 (giving an example of how, when the OPM was attacked, it caused harm to other connected organizations because of a security weakness showing that any company or federal agency associated with another is at risk when a hacking occurs).

259. Nuala O'Connor, *Our Personal Security Is Our National Security*, THE HILL (Mar. 1, 2016, 11:00 AM), http://thehill.com/blogs/congress-blog/homeland-security/271181-our-personal-security-is-our-national-security. O'Connor is the current President & CEO of the Center for Democracy & Technology. She is the former Chief Privacy Officer for the Department of Homeland Security, the inaugural person to fill that role. *Nuala O'Connor, President & CEO*, CTR. FOR DEMOCRACY & TECH., https://cdt.org/about/staff/nuala-o%E2%80%99connor/ (last visited Oct. 26, 2016).

260. One possible scenario is that hackers could get into U.S. government computers and then send false requests to the team. Another possible scenario is that an insider could be compromised and subsequently abuse their position. Abelson et al., *supra* note 6, at 2.

261. *Id*.

262. *Id*.

263. *See* BERKMAN CTR. FOR INTERNET & SOCIETY, HARV. UNIV., DON'T PANIC: MAKING PROGRESS ON THE "GOING DARK" DEBATE (2016), https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf (questioning the "going dark" FBI approach by questioning whether the ability to surveil criminals and bad actors will be impossible and determining that would not be the case).

264. According to the authors of *Don't Panic*, factors includes the combination of technological developments and market forces (think: targeted advertising), and the "prevalence of network sensors and the "Internet of Things." *Id*. at 19.

265. *See id*. at 2 (arguing that the market will cause an increase in unencrypted data, filling the encryption gaps that governmental agencies such as the FBI assume will go dark in the future).

furthermore, there are opportunities to fill in the gaps by other measures. This argument is supported by the Chertoff Group's *Ground Truth* white paper, in its assertion that "we can find no successful terrorist attack that would have been prevented by the availability of a lawful decryption access technology."[266]

As explained in *Keys Under Doormats*, and expounded upon by Mr. Schneier and the *Motherboard* article, changing course and demanding access to encryption would make personal information less safe. Many daily activities utilize encryption technology, such as online banking, shopping, and emails (personal and professional). These sensitive sets of information are best served by the most secure systems possible. And when viewed with the perspective of the intrusive regulations and laws being passed in other nations, allowing for strong encryption would make us comparatively safer because our personal information would be secure.

As a result of the already changed or currently changing legislation in other nations, the U.S. finds itself in a unique and potentially advantageous position. By not acting to regulate end-to-end encryption, the U.S. could actually make itself comparatively safer than other nations. Other countries have made their citizens more vulnerable to hacking or cyber-attacks as a result of the countries' regulations. By not regulating, the U.S. retains its level of security and stature in the global tech market while simultaneously becoming more secure. *Ground Truth* quotes General Michael Hayden as saying,[267] "[b]ecause of the nature of global telecommunications, we are playing with a tremendous home-field advantage, and we need to exploit that edge. . . ."[268]

Having this built in "home-field" advantage over tech companies should be a boon to the American economy and national security. It would keep capital and innovation within American borders. In addition, the metadata that is associated with the encrypted data that passes through the U.S. will likely continue to do so if encryption remains strong. For example, Brazil has announced that the nation plans to build Internet cables that go under the Atlantic Ocean to reach Portugal.[269]

---

266. *The Ground Truth About Encryption and the Consequences of Extraordinary Access*, THE CHERTOFF GROUP 2 https://chertoffgroup.com/cms-assets/documents/238024-282765.groundtruth.pdf (last visited Oct. 18, 2016) [hereinafter *Ground Truth*]. In the interest of completeness, *Ground Truth* continues on ". . .but in the future it is likely that ubiquitous encryption will have an impact on law enforcement capabilities." *Id*. This is contradictory to the central thesis of *Don't Panic* that ubiquitous encryption is unlikely to occur due to certain market forces. Mr. Chertoff, the founder of the Chertoff Group, is the former Secretary of Homeland Security, during the George W. Bush Administration. He was also formerly a Federal Judge on the Third Circuit Court of Appeals. *The Honorable Michael Chertoff*, THE CHERTOFF GROUP https://chertoffgroup.com/bios/michael-chertoff.php (last visited Oct. 18, 2016).

267. General Hayden is the former Director of the NSA and the CIA. He was also the Principal Deputy Director of National Intelligence, amongst other prestigious posts in the Defense and Intelligence sectors. He is currently a Principal in the Chertoff Group. *Michael Hayden*, THE CHERTOFF GROUP https://chertoffgroup.com/bios/michael-hayden.php (last visited Oct. 18, 2016).

268. *Ground Truth*, *supra* note 266, at 17.

269. *See id*. at 17–18 (stating that the cables will cost $185 billion).

Brazil plans to do this to avoid U.S. regulations on data collection.[270] If the U.S. regulates encryption, it would take away both the capital associated with the existing Brazilian communications passing through the U.S. as well as the metadata associated with the encrypted data. Thus, if the U.S. wants to maintain its "home-field" advantage, it should not pass heavy-handed regulation of encryption technology.

VIII. CONCLUSION

The state of confusion created around the issue of encryption is a result of diverging methods of regulation around the world and differing views of the utility of the technology within the U.S. government.[271] All of these divergent stances and policies ultimately make global networks less secure and thus make American information and data less safe. However, the U.S. is in a unique position as a global leader in both innovation and in the transportation of communication. Encryption makes data more secure and makes countries safer from hackers and terrorists. The U.S. should defer to the tech industry's knowledge on encryption, as doing so will make its data and its communication systems comparatively more secure, which will increase personal and national security. The creators of these encrypted systems know the consequences of compromising the systems' integrity better than anyone else and the relevant actors concerned with this issue should defer to their positions. Choosing between security of encrypted networks and an efficient and complete effort against crime and terror is a false choice.

270. *Id*.

271. *See*, Cushing, *supra* note 221 (providing a pertinent example of the lack of a unified front on encryption between the Department of Defense, the NSA, and the FBI, three of the key players in security).