ENCRYPTION SERVED THREE WAYS: DISRUPTIVENESS AS THE KEY TO EXCEPTIONAL ACCESS

Dustin Taylor Vandenberg†

Recently, there has been a rapid increase in the deployment of encryption technologies.[1] While the ubiquity of encryption has led to innovations in security and privacy,[2] these benefits stand at odds with government interests in access to data.[3] Controversial court cases in San Bernardino[4] and New York[5] highlight the modern debate over exceptional access to encrypted data. However, the debate over encryption is not new. The debate began back in the 90s in what has been dubbed the "crypto

DOI: https://dx.doi.org/10.15779/Z38GT5FF7R

† J.D. Candidate, 2018, University of California, Berkeley, School of Law.

1. *See* Susan W. Brenner, *Intellectual Property Law Symposium: Encryption, Smart Phones, and the Fifth Amendment*, 33 WHITTIER L. REV. 525, 533 (2012) ("I believe we will see an increased use of encryption and other data-protection measures that will make it increasingly difficult, if not impossible, for officers to access the contents of a smart phone or other digital device by bypassing minimal, if any, security measures."); *see also, e.g.*, Craig Timberg, *Newest Androids Will Join iPhones in Offering Default Encryption, Blocking Police*, WASH. POST BLOG (Sept. 18, 2014) ("The next generation of Google Android's operating system . . . will encrypt data by default.") https://www.washingtonpost.com/news/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/?utm_term=.0800c87af627 [https://perma.cc/S7ZS-J9XP].

2. H Abelson et al., *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, MASS. INST. OF TECH. COMPUT. SCI. & ARTIFICIAL INTELLIGENCE LAB. 5 (2015) ("After lengthy debate and vigorous predictions of enforcement channels 'going dark,' these attempts to regulate the emerging Internet were abandoned. In the intervening years, innovation on the Internet flourished.").

3. *See, e.g.*, MAJORITY STAFF OF H. HOMELAND SEC. COMM., 114TH CONG., GOING DARK, GOING FORWARD: A PRIMER ON THE ENCRYPTION DEBATE (2016), http://homeland.house.gov/wp-content/uploads/2016/07/Staff-Report-Going-Dark-Going-Forward.pdf [https://perma.cc/6ALL-QHE8] [hereinafter GOING DARK, GOING FORWARD].

4. *In the Matter of the Search of an Apple IPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, CA License Plate 35 KGD203,* No. ED-0451M, 2016 WL 618401 (C.D. Cal. Feb. 16, 2016).

5. *In re Apple, Inc.*, 149 F. Supp. 3d 341 (E.D.N.Y. 2016).

wars."[6] While the initial round of the crypto wars was won by proponents of strong cryptography, difficult questions still remain. Recently, the debate over cryptography has reignited over exceptional access to encrypted data. Some recently proposed policies regarding exceptional access have been broad and unclear in their scope.[7]

In order for the debate over exceptional access to encryption to move forward, it is important to understand the three primary contexts where encryption is used: data in the cloud, data in-transit, and data on endpoint devices. This Note seeks to provide some clarity as to how policymakers can include these nuances in their discussions on encryption. Policymakers should carefully consider the technology underpinning encryption, the usage of encryption, and the risks associated with exceptional access to encrypted data—a combination called "disruptiveness."

Part I will cover some of the necessary technical background on encryption to frame the discussion. Part II proposes a new framework to the debate over exceptional access, focusing on the disruptiveness that exceptional access would have on each of the three major implementations of encryption. Part III applies this framework in the cloud context. Part IV examines data-in-transit. Part V analyzes data at rest on endpoints. Finally, Part VI looks to the potential future of the debate over exceptional access with disruptiveness in mind.

I. WHAT ARE ENCRYPTION AND EXCEPTIONAL ACCESS?

Before diving into the debate, it is important to have a clear idea what encryption and exceptional access are and how they work.

A. ENCRYPTION

In order to distinguish among various implementations of encryption, it is necessary to understand what encryption is. In the most basic sense,

6. *See* Urs Gasser et al., *Don't Panic. Making Progress on the "Going Dark" Debate* at 5, BERKMAN CTR. FOR INTERNET & SOC'Y AT HARV. UNIV. (2016).

7. Draft language of the Compliance with Court Orders Act of 2016 requires that companies provide "information or data" to the government in an "intelligible format" or provide "technical assistance as is necessary to obtain such information or data." Compliance with Court Orders Act of 2016, S.___, 114th Cong. § 3(a)(1) (Discussion Draft 2016) [hereinafter Compliance with Court Orders Act], http://www.feinstein.senate.gov/public/_cache/files/5/b/5b990532-cc7f-427f-9942-559e73eb8bfb/6701CF2828167CB85F51D12F7CB69D74.bag16460.pdf [https://perma.cc/F2Q4-2G93]; *see also* GOING DARK, GOING FORWARD, *supra* note 3, at 6 ("Any legislative 'solutions' yet proposed come with significant trade-offs, and provide little guarantee of successfully addressing the issue.").

encryption is a method of taking readable data (called "plaintext") and "scrambling" it into a ciphertext that is unreadable.[8] Encryption requires a "key," which effectively tells the encryption process how to "scramble" the data.[9] Decryption is the opposite of encryption, taking that "scrambled" ciphertext and turning it back into a readable format.[10] In order for the data to be readable, typically, the decryption algorithm must use the exact same key as the encryption process.[11]

Data can be stored either at-rest or in-transit. Data at-rest is data that is sitting on one device (such as a laptop, phone, or server).[12] Data in-transit is data being sent among two or more devices.[13] When one encrypts data, one must be sure that the key is only shared with individuals who should be allowed to decrypt that data.[14] For data in-transit, this requires that the two communicating parties know a shared secret key so that the parties can encrypt and decrypt each other's communications.[15] Because both parties must have the exact same key, encryption of data in-transit using a shared secret key is typically referred to as "symmetric encryption."[16]

One of the major difficulties in using symmetric encryption is that two parties must therefore have a method to exchange the private key. Throughout the history of cryptography, this posed the risk that anyone eavesdropping on their conversation would be able to determine what their shared private key was.

This problem was solved using what is called a Diffie-Hellman key exchange.[17] This exchange requires that each party has two keys, one public and one private.[18] The public and private keys from each party are combined so that both of the parties end up with the same shared private session key,

8. SERGE VAUDENAY, A CLASSICAL INTRODUCTION TO CRYPTOGRAPHY: APPLICATIONS FOR COMMUNICATIONS SECURITY 21 (2006).

9. *Id.*

10. *Id.*

11. BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C 2–3 (1994).

12. Dave Shackleford, *Regulations and Standards: Where Encryption Applies* at 2, SANS INST. INFOSEC READING ROOM (2007), https://www.sans.org/reading-room/whitepapers/analyst/regulations-standards-encryption-applies-34675 [https://perma.cc/RA28-9LFW].

13. *Id.*

14. KLAUS SCHMEH, CRYPTOGRAPHY AND PUBLIC KEY INFRASTRUCTURE ON THE INTERNET 42–43 (2003).

15. SCHNEIER, *supra* note 11, at 2–3.

16. SCHMEH, *supra* note 14, at 42–43.

17. *See* Whitfield Diffie & Martin E. Hellman, *New Directions in Cryptography*, 22 IEEE TRANSACTIONS ON INFO. THEORY 644 (1976).

18. SCHNEIER, *supra* note 11, at 29–30.

which is essentially a mix of both parties' private and public keys.[19] An adversary who did not know the private keys of both parties would be unable to replicate the "mix" and determine what that shared private key is, even if the adversary saw all the communications between the two parties.[20] Because this method requires that both parties begin with two distinct keys, one public and one private, it is referred to as "asymmetric encryption."[21]

B. EXCEPTIONAL ACCESS

Exceptional access is giving an individual or organization (often the Government) access to the readable data someone has encrypted. Exceptional access requires that the third party be granted access to the plaintext data associated with encrypted data.[22] Exceptional access to communications requires one of the following: key escrow,[23] key generation vulnerabilities,[24] brute-force attacks,[25] or a vulnerability known as a "zero-day."[26]

Under key escrow, each individual communication still uses a private key to encrypt the data, but that key is stored in escrow.[27] Under this scheme, when the government needs access to encrypted content, the government would get the secret key from the key escrow and use that key to decrypt the data at issue.[28]

A second method of exceptional access is to introduce a vulnerability into the key generation process. Virtually all key generation in cryptography relies upon pseudo-random number generators.[29] When two parties want to communicate, the parties use these generators to create random keys that

19. SCHMEH, *supra* note 14, at 94–95.

20. *Id.*

21. VAUDENAY, *supra* note 8, at 229.

22. K. W. Dam et al., *Cryptography's Role in Securing the Information Society*, NAT'L ACAD. PRESS 80 (1996) ("Exceptional access refers to situations in which an authorized party needs and can obtain the plaintext of encrypted data.").

23. *Id.* at 167 ("Escrowed encryption is the basis for a number of Administration proposals that seek to reconcile needs for information security against the needs of law enforcement and to a lesser extent national security.").

24. SCHNEIER, *supra* note 11, at 140–145 ("[An attacker] doesn't have to attempt to cryptanalyze your cryptographic algorithm when [they] can cryptanalyze your key generation algorithm.").

25. VAUDENAY, *supra* note 8, at 51-62.

26. ROBERT O'HARROW, ZERO DAY: THE THREAT IN CYBERSPACE 7 (2013) (a 'zero day' is "a vulnerability in the software that has never been made public and for which there is no known fix").

27. K. W. Dam et al., *supra* note 22, at 80.

28. *Id.*

29. SCHNEIER, *supra* note 11, at 39–41.

are then used to generate the shared private key.[30] If a third party were able to replicate that random number generation, the third party could follow the same publicly-known steps as the parties to gain access to the same shared private key.[31] Under this scheme, the pseudo-random number generators would need to allow the government to replicate the random number generation used by the communicating parties at the time of key generation; that way the government could replicate the process using those mandated generators.

There are other approaches that do not fully satisfy governmental interests. An actor seeking access may simply guess passwords until the correct key is obtained, bypassing the protections afforded by encryption. This process is known as a "brute-force" attack.[32] In cases with short passwords, such as 4-digit PINs on phones, this may be an effective solution. However, brute-force attacks may be impractical depending on the length and complexity of the password and the design of the cryptographic system.[33]

Another partial solution for specific cryptographic products is using an unintended vulnerability known as a "zero-day." By definition, a zero-day is a vulnerability that has not yet been exposed or patched.[34] This is the vulnerability the FBI used to gain access to the San Bernardino shooter's iPhone.[35] Using zero-day vulnerabilities may not, however, be a practical solution for day-to-day operations in law enforcement and intelligence. The San Bernardino zero-day, for example, reportedly cost over $1,300,000

30. *See* SCHMEH, *supra* note 14, at 134–39 (describing commonly implemented generators using feedback functions, cryptographic hash functions, and linear feedback shift registers).

31. *Id.*

32. SCHNEIER, *supra* note 11, at 129–136.

33. Complex PINs longer than a few digits or passwords containing a variety of letters, numbers, or symbols may take hundreds of millions of years of computing time to guess, even without any delay imposed by the hardware or software; however, shorter passwords and dedicated brute-force hardware may be able to reduce this computing time depending on the protocols utilized. *See Id.*

34. These vulnerabilities are called "zero-days" because there have been zero days since the vulnerability was released to the public, making them highly valuable and extremely effective because no patch exists to prevent the vulnerability. *See* O'HARROW, *supra* note 26, at 7.

35. Ellen Nakashima, *FBI Paid Professional Hackers One-Time Fee to Crack San Bernardino iPhone*, WASH. POST (April 12, 2016), https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html?utm_term=.c79030c4e81f [https://perma.cc/46T9-RKLC].

alone and may not work on phones with different versions of iOS or different hardware.[36]

II. MAKING PROGRESS ON EXCEPTIONAL ACCESS THROUGH DISRUPTIVENESS

One of the first battles in the "crypto wars" involved a device known as the "Clipper Chip."[37] In 1993, as cryptography transitioned from military and government use to consumers and corporations, there was a fear that the government would be locked out of crucial communications. In response, the NSA designed a small computer chip, which manufacturers would implement into electronics throughout the United States.[38] The chip was designed to contain a government master key that could provide access to encrypted communications when legally appropriate.[39] This key escrow system was met with intense criticism by civil libertarians and technologists. There were concerns over the security implications of the clipper chip,[40] the impact on innovation in cryptography,[41] and the effects on privacy.[42] As a result of this backlash, the clipper chip proposal died.[43]

Jumping forward to today, Congress has begun to discuss legislative solutions to provide exceptional access to encrypted data in light of the battle between Apple and the FBI. In the last Congress, draft legislation known as "The Compliance with Court Orders Act of 2016" would have required that companies provide "information or data" to the government in an "intelligible format" or provide "technical assistance as is necessary to obtain such information or data."[44] This proposal was met with resistance

36. Tom Spring, *Experts Weigh-In Over FBI $1.3 Million iPhone Zero-Day Payout*, THREATPOST (April 22, 2016), https://threatpost.com/experts-weigh-in-over-fbi-1-3-million-iphone-zero-day-payout/117614/ [https://perma.cc/93UK-TR38].

37. H Abelson et al., *supra* note 2, at 5.

38. *Id.*

39. *Id.*

40. *See e.g.,* Matt Blaze, *Protocol failure in the Escrowed Encryption Standards*, AT&T BELL LABS. (1994).

41. *See, e.g.,* LANCE J. HOFFMAN, BUILDING IN BIG BROTHER 393-399 (1995).

42. *See, e.g.,* Marc Rotenberg et al., *Crypto Experts Letter on Clipper* (Jan. 1994), https://epic.org/crypto/clipper/crypto_experts_letter_1_94.html [https://perma.cc/TJ3D-QM2B].

43. Parker Higgins, *On the Clipper Chip's Birthday, Looking Back on Decades of Key Escrow Failures*, ELECTRONIC FRONTIER FOUND. (April 16, 2015) (Blog post), https://www.eff.org/deeplinks/2015/04/clipper-chips-birthday-looking-back-22-years-key-escrow-failures [https://perma.cc/25Z4-XHS2].

44. Compliance with Court Orders Act of 2016, S.___, 114th Cong. § 3(a)(1) (Discussion Draft 2016).

from industry and advocacy groups such as the Information Technology and Innovation Foundation,[45] the Internet Association,[46] and the Electronic Frontier Foundation,[47] as well as from elected officials.[48] This proposal did not distinguish among differing forms of encryption,[49] rending it overly broad and unrealistic to implement.[50] Because of some of these criticisms, the bill was not enacted.[51]

A. ENCRYPTION IN THE LEGAL SPHERE

At a federal level, encryption has played a large role in debates surrounding access to digital communications. The Communications Assistance for Law Enforcement Act (CALEA) of 1994 required that telecommunications carriers ensure that the government could, with lawful

45. Daniel Castro, *Compliance with Feinstein-Burr Encryption Bill Would Create Untenable Legal Paradox for U.S. Companies*, INFO. TECH. AND INNOVATION FOUND. (2016) ("In short, this bill sets up a legal paradox that would further muddy the waters about how and when the government can compel the private sector to assist in gaining access to private information").

46. Michael Beckerman, *Statement on the Compliance with Court Orders Act of 2016*, INTERNET ASS'N (Apr. 11, 2016). The statement read, in part:

> The draft legislation, as currently written, creates a mandate that companies engineer vulnerabilities into their products or services, which will harm national security and put Americans at risk. Strong encryption is vital to protecting national security, personal privacy, communications, the electric grid, hospitals, and our defense systems. Mandating the weakening of encryption will put the United States' national security and global competitiveness at risk without corresponding benefits. As the Administration considers its response to the bill, we hope President Obama takes a position that supports the use of strong encryption without backdoors.

47. Patrick Howell O'Neill, *EFF Vows to Tie Up Encryption 'Backdoor' Legislation in Court 'For Years,'* DAILY DOT (Apr. 8, 2016) ("The first thing that's going to happen is that any backdoor legislation is going to be tied up in the courts for years . . . . The EFF is going to lead that effort.").

48. *See, e.g.*, Ron Wyden, *Wyden Statement on Burr-Feinstein Anti-Encryption Bill* (April 13, 2016) ("Americans who value their security and liberty must join together to oppose this dangerous proposal. I intend to oppose this bill in committee and if it reaches the Senate floor, I will filibuster it.").

49. *See* Compliance with Court Orders Act of 2016, S.___, 114th Cong. § 4(5)(B) (including "information stored remotely or on a device provided, designed, licensed, or manufactured by a covered entity" in the definition of "data," thus failing to distinguish between data on an endpoint versus data in the cloud.).

50. Cindy Cohn, *The Burr-Feinstein Proposal is Simply Anti-Security*, ELECTRONIC FRONTIER FOUND. (Apr. 8, 2016).

51. Dustin Volz et al., *Push for Encryption Law Falters Despite Apple Case Spotlight*, REUTERS (May 27, 2016).

authorization, intercept wire and electronic communications.[52] In 2005, CALEA was expanded to cover voice over internet protocol (VoIP) service;[53] however, CALEA states that telecommunication carriers are not "responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication."[54]

Encryption has also worked its way into regulatory frameworks surrounding cybersecurity best practices. While not always explicitly required, agencies like the Federal Trade Commission (FTC) have found security measures to be unreasonable, in part, because of a lack of encryption utilization.[55] Furthermore, state legislatures have viewed encryption as an important safeguard against data breaches, with many states incorporating "safe harbors" to data breach notification requirements when companies encrypt their data.[56]

Finally, the courts have recognized the extensive personal information which is available on many consumer electronic devices, which may pave the way for stronger privacy protections through encryption.[57] Conversely, there are a number of pending cases that exemplify the risks law enforcement face when key evidence is locked away with encryption.[58]

B. THE CULTURAL BATTLE BEHIND ENCRYPTION

A cultural battle between the technology community and the legal/policy community must be recognized in this debate. At a fundamental

52. 47 U.S.C. § 1002(a) (1994).

53. *See* Fed. Commc'ns Comm., *In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services*, 20 FCC Rcd. 14989 (Sept. 2005).

54. 47 U.S.C. § 1002(b) (1994). As an aside, it is unclear whether this exemption would protect carriers who do encrypt and *could* possess the information necessary to decrypt, but choose not to keep encryption keys used by their customers, as is the case with forward secrecy.

55. *See* Complaint at 2, *In Re BJ's Wholesale Club, Inc.*, No. 042 3160 (F.T.C. 2005).

56. Baker & Hostetler LLP, *Data Breach Charts* (2016), https://www.bakerlaw.com/files/uploads/documents/data%20breach%20documents/data_breach_charts.pdf [https://perma.cc/BKW9-WQ8C] (showing as of January 1, 2017, 49 states and territories grant some form of encryption safe harbor).

57. *See Riley v. California*, 134 S. Ct. 2473 (2014), which is discussed in greater detail *infra* Section V.C.3.

58. *See, e.g., People v. Sandel, Rivera, and Cruz*, Indictment No. 3158/15 (N.Y. Sup. Ct. 2015) (rape and robbery conspiracy); *People v. Hirji*, Indictment No. 3650/15 (N.Y. Sup. Ct. 2015) (child pornography); *People v. Brown*, Indictment Nos. 865/12, 3908/12, and 3338/13 (N.Y. Sup. Ct. 2013) (sex trafficking); *People v. Rosario*, Indictment No. 1859/10 (N.Y. Sup. Ct. 2010) (homicide exoneration).

level, these two groups see encryption and government access to data through very different lenses.

The prototypical Silicon Valley technologist sees technology and innovation as the keys to progress. Computer code should be written to be bug free and secure.[59] From this viewpoint, any vulnerability in encryption goes against the fundamental principle that drives Silicon Valley forward: innovation. In this mindset, innovations in security are what have created the secure communications[60] which underpin the U.S. economy.[61] Exceptional access asks these technologists to abandon this progress and leave their customers with a product that is less secure than current technology allows, which is extremely unappealing. This side of the debate believes the government's demands are unnecessary, as the proliferation of

59. *See, e.g.,* Apple, *iOS Security Guide: iOS 9.3 or Later* at 18 (May 2016) ("[Apps are] reviewed by Apple to ensure they operate as described and don't contain obvious bugs or other problems . . . [which] gives customers confidence in the quality of the apps they buy."); Brief of the Center for Democracy & Technology as *Amicus Curiae* in Support of Apple Inc.'s Motion to Vacate and in Opposition to Government's Motion to Compel Assistance at 2, *In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203* (2016) (ED No. CM 16-10 (SP)) ("[S]ystems need to be safe from malicious third party attacks. A decision compelling Apple to weaken critical security features on its phones will leave [consumers] . . . vulnerable. Companies . . . work hard to make [their technology] secure."); Brief of *Amicus Curiae* AirBnB, Inc.; Atlassian Pty. Ltd.; Automattic Inc.; Cloudflare, Inc.; eBay Inc.; Github, Inc.; Kickstarter, Pbc; LinkedIn Corporation; Mapbox Inc.; A Medium Corporation; Meetup, Inc.; Reddit, Inc.; Square, Inc.; Squarespace, Inc.; Twilio Inc.; Twitter, Inc.; and Wickr Inc. at 4, *In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203* (2016) (ED No. CM 16-10 (SP)). According to this brief:

> The increasing ubiquity of the Internet in all aspects of life has ushered in a new generation of innovative products and services for consumers and businesses. In the midst of this digital revolution—and the ever-present and increasing dangers posed by hackers, identity thieves, and other wrongdoers—ensuring that users' data is handled in a safe, secure, and transparent manner that protects privacy is of utmost importance.

60. Brief of *Amicus Curiae* AirBnB, Inc., *supra* note 59, at 4 ("These services provide the ability to communicate with friends, family, colleagues, external advisers and the world at large; to share and read live news from around the world or in-depth works of commentary and expression.").

61. *Id.* ("For the companies operating in today's ever-connected digital world, the values of privacy, security, and transparency are essential guiding principles for building trust with their users.").

devices and communications has placed us in the "golden age of surveillance."[62]

Meanwhile, a completely different mindset can be found in the law enforcement and intelligence community. While those advocating for exceptional access can understand the importance of encryption to computer security, their profession revolves around managing risk, not eliminating it.[63] Decisions are based upon comparing a wide array of less-than-ideal solutions to try and minimize harms and maximize benefits. From this viewpoint, this sort of balancing is required to meet the operational goals of protecting our communities and national security.[64] The government fears that the continued proliferation of encryption will lead to a future where access to key evidence[65] and intelligence[66] is impossible, a fear known as "going dark."[67] To advocates on this side, cases like San Bernardino are just the tip of the iceberg, as more and more devices are

62. *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy*: *Hearing Before the S. Comm. On the Judiciary*, 114TH CONG. (2015) (statement of Prof. Peter Swire).

63. Jonathan Remy Nash, *The Supreme Court and the Regulation of Risk in Criminal Law Enforcement*, 92 B.U. L. REV. 171, 178 ("Insofar as it involves risk to alleged criminals, convicted criminals, the public, and law enforcement officers, criminal law enforcement raises a host of risk-related issues.").

64. Brief of *Amici Curiae* Federal Law Enforcement Officers Association, Association of Prosecuting Attorneys, Inc., and National Sheriffs' Association in Support of the Government's Motion to Compel Apple, Inc. to Comply with This Court's February 16, 2016 Order Compelling Assistance in Search at 2, *In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203* (2016) (ED No. CM 16-10 (SP)). The *Amici* members are:

> [C]alled upon on a daily basis to protect and serve the public by investigating criminal activity and wrongdoing to ensure that the individuals responsible for it pay the penalty for their crimes. In order to fulfill their duties, *Amici* members must have access to all reasonable means of procuring relevant evidence.

65. *See* Manhattan Dist. Attorney's Office, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety* at 9–12 (November 2015) (discussing cases where encryption rendered evidence unavailable for homicides, rape and robbery conspiracy, child pornography, sex trafficking, cybercrime and identity theft, and unlawful surveillance).

66. MAJORITY STAFF OF H. HOMELAND SEC. COMM., *supra* note 3, at 10 ("[L]aw enforcement and intelligence officials have reported to Committee staff that their inability to obtain access to the digital communications of criminals is increasingly hindering their activities . . . Unfortunately, terrorists also use encryption technology to hide their communications from law enforcement and intelligence professionals.").

67. *Encryption Tightrope: Balancing Americans' Security and Privacy*, 114TH CONG. 9–13 (2016) (statement of James B. Comey, Director of Federal Bureau of Investigation).

becoming unreachable[68] despite having a legal right to access the data on the device. Advocates on this side contend that the rationales for ubiquitous encryption may be overstated and misleading.[69] They argue, on balance, that these concerns may not outweigh the societal costs associated with a lack of access to evidence and intelligence.[70]

C. A BETTER WAY FORWARD: DISRUPTIVENESS ON THREE FRONTS

Past attempts to address the issue of exceptional access (such as the Clipper Chip or the Compliance with Court Orders Act) teach valuable lessons for future attempts to forge compromise. Rather than attempting to broadly address all encryption, proposals should be tailored. Encryption is deployed in three very different contexts, and moving forward, policymakers should recognize how these varying implementations can entail differing technologies, incentives, and risks. Without this context on the forefront of the discussion, future policy proposals are likely to meet the same fate as their predecessors.

This Note proposes viewing the "disruptiveness" of exceptional access as a way to compare exceptional access in the cloud, in-transit, and in endpoints. While the phrase "disruptiveness" is a somewhat broad metric, the extensive nature of this problem requires a metric broad enough to

---

68. *Id.*

69. *See Government's Motion to Compel Apple Inc. to Comply with This Court's February 16, 2016 Order Compelling Assistance in Search* at 6-7, *In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203* (2016) (ED No. CM 16-10 (SP)) ("Apple appears to object based on a combination of: a perceived negative impact on its reputation and marketing strategy were it to provide the ordered assistance to the government, numerous mischaracterizations of the requirements of the Order, and an incorrect understanding of the All Writs Act."); *see also Amicus Curiae* Brief of Greg Clayborn, James Godoy, Hal Houser, Tina Meins, Mark Sandefur, and Robert Velasco at 6, *In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203* (2016) (ED No. CM 16-10 (SP)) ("Apple is conflating many different policy debates for the dual purposes of excusing itself from compliance with current law and protecting its public image.").

70. *See* Manhattan Dist. Attorney's Office, *supra* note 62, at 2–3. The report states:

> Previous Apple and Google operating systems allowed law enforcement to access data on devices pursuant to search warrants. There is no evidence of which we are aware that any security breaches have occurred relating to those operating systems. Apple and Google have never explained why the prior systems lacked security or were vulnerable to hackers, and thus, needed to be changed. Those systems appeared to very well balance privacy and security while still being accessible to law enforcement through a search warrant.

encompass the various aspects of the debate.[71] Disruptiveness can, in a basic sense, be thought of as a combination of two separate measurements: (1) the extent that encryption is used in a particular context and (2) the risks associated with exceptional access in that context.

These measurements should be viewed with an eye toward the unique aspects of encryption technology in the differing contexts of the cloud, in-transit, and endpoints. Unless the debate recognizes these nuances, proposals may lack clarity and create technically infeasible requirements.

1. Extent of Use of Encryption

The first factor of disruptiveness examines how prevalent the use of encryption is within a given context. After all, if encryption is not widely deployed in a particular context, then a mandate that potentially undermines the effectiveness of that encryption may not disrupt as many individuals. However, it is important to note not only the current utilization of encryption, but also the trends moving forward. Even if encryption is minimally deployed within a particular context, efforts to undermine encryption may serve to chill future use of encryption—which can increase the disruptiveness in that context.

2. Risks of Exceptional Access

When evaluating the risks associated with mandating exceptional access within a particular context of encryption, there are four key factors to assess: (1) Within that context, what threats are faced? (2) How does encryption respond to those threats? (3) Would exceptional access undermine those protections? (4) Can alternatives to encryption also respond to the threats?

This framework provides consistency in the analysis among the various contexts where encryption is used while taking into account the fundamental purposes behind having encryption in the first place. If there are alternatives to encryption that can provide similar protections, then a mandate of exceptional access may have limited disruptiveness.

D. THE IMPLICATIONS OF DISRUPTIVENESS

Finally, even if there is a clear idea of how "disruptive" exceptional access is in a given context the natural next question is: what are the implications of that level of disruptiveness? By-and-large, disruptiveness

71. Exceptional access implicates issues with cybersecurity, innovation, law enforcement, national security, privacy, human rights, technical interoperability, consumer interests, corporate interests, international relations, and more. This Note will provide only a limited contribution towards the full understanding of how disruptive exceptional access may be in various contexts.

can serve as a guide to help guide progress in the debate over exceptional access. As a general rule, areas where exceptional access would be less disruptive are likely better avenues for debate—as the negative ramifications of exceptional access are lessened.

However, this disruptiveness must also be balanced against the various needs for exceptional access in each of the three contexts of encryption. If, for instance, the need for exceptional access to endpoint devices is significantly greater for law enforcement and intelligence when compared to data in-transit or in the cloud, then that need should be counterbalanced against the disruptiveness to provide a comparison between exceptional access in each separate context.

Currently, however, it is unclear if there are reasons why the government (if it were forced to prioritize) would choose any one particular context over another. Given the diversity in missions and resources between local law enforcement, federal law enforcement, domestic intelligence agencies, and foreign intelligence agencies, it can be difficult to define what "the government" as a whole even wants when it comes to exceptional access, short of "everything."

Encryption on endpoint devices can limit access both to devices for local law enforcement's evidence gathering in a murder case[72] and access to key intelligence recovered from raids on terrorist networks overseas.[73] Likewise, intelligence agencies may use monitoring of internet messages and e-mails to help investigate and stop criminal activity and national security threats.[74] Furthermore, warrants to search data stored by cloud

---

72. *See* Manhattan Dist. Attorney's Office, *supra* note 62, at 9. *People v. Hayes*, Indictment Number 4451/12:

> The victim was filming a video using his iPhone when he was shot and killed by the defendant. The video captured the shooting. Because the iPhone was not passcode-locked, the video was recovered and admitted into evidence at trial. The video corroborated eyewitness testimony. The defendant was convicted of murder and sentenced to 35 years to life.

73. *See* Emily Rand, *Source: 2.7 terabytes of data recovered from bin Laden compound*, CBS NEWS (May 6, 2011), http://www.cbsnews.com/news/source-27-terabytes-of-data-recovered-from-bin-laden-compound/ [https://perma.cc/D7L3-X4NQ]. A law enforcement source told CBS News that "2.7 terabytes of data were recovered from the laptops, computers, hard drives and other storage devices seized from the bin Laden compound . . . Sources said much of the material seized in the daring raid was encrypted so the messages could not be read if they were intercepted."

74. *See* Charlie Savage & Nicole Perlroth, *Yahoo Said to Have Aided U.S. Email Surveillance by Adapting Spam Filter*, N.Y. TIMES (Oct. 5, 2016), https://www.nytimes.com/2016/10/06/technology/yahoo-email-tech-companies-government-investigations.html [https://perma.cc/8EZT-2SX2]. According to this article:

providers like Facebook may be key for law enforcement at all levels.[75] It is difficult to guess which of these missions is the most important and would be prioritized, as all can be crucial to advancing the mission of various government agencies.

Moving forward, clarity on where exactly the need for exceptional access is greatest would help inform and potentially counterbalance disruptiveness. Given the limited scope of this Note, until the prioritization of these contexts by the government is clear, we can operate on the assumption that the government treats all forms of encryption and all sources of data as roughly equivalent in importance. Therefore, disruptiveness acts as the primary differentiator between progress on exceptional access to encrypted data in the cloud, in-transit, or at endpoints.

In this Note, disruptiveness is roughly scored on a scale from low to medium to high. Where exceptional access is highly disruptive, policymakers should be wary of mandating exceptional access, as the costs (monetary, security, public perception, privacy, etc.) will likely outweigh any benefits that exceptional access may provide; however, where disruptiveness is low or medium, there is more potential for a meaningful compromise which can allow government access while protecting the security of computer systems within that context.

III. ENCRYPTION IN THE CLOUD

First, we can examine the potential disruptiveness of exceptional access to encrypted data stored in the cloud. Here, there has been limited adoption of encryption technology, yet encryption can be effective at protecting some

> Yahoo customized an existing scanning system for all incoming email traffic, which also looks for malware . . . [T]he system stored and made available to the Federal Bureau of Investigation a copy of any messages it found that contained the digital signature . . . Investigators had learned that agents of the foreign terrorist organization were communicating using Yahoo's email service and with a method that involved a 'highly unique' identifier or signature.

75. *See* LEXISNEXIS, SOCIAL MEDIA USE IN LAW ENFORCEMENT 2 (2014), https://www.lexisnexis.com/risk/downloads/whitepaper/2014-social-media-use-in-law-enforcement.pdf [https://perma.cc/9JV4-BHRV]. The report states:

> Law enforcement professionals throughout the U.S. are increasingly turning to modern technology, including social media, to aid in carrying out their public safety mission, with a primary goal of preventing and investigating crime. The frequency of social media use by law enforcement, while already high, is projected to rise even further in the coming years.

cloud systems. Therefore, the disruptiveness is somewhere between low and medium.

A. CLOUD TECHNOLOGY AND DEPLOYMENT MODELS

The National Institute of Standards and Technology defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) . . ."[76] Generally speaking, this means that cloud computing is an internet-based service for users to access software, resources, and information stored elsewhere and managed by someone else. [77] However, the exact technical implementation of a cloud depends on the deployment model of the cloud provider. There are four types of cloud deployment models: private, community, public, and hybrid. [78]

A private cloud model requires that the cloud services are used by a single organization.[79] A public cloud model provides a service to the general public and gives the cloud provider full control of the cloud services. [80] A community cloud model provides cloud services to a number of organizations which are jointly managed by a single provider. [81] A hybrid model combines any of the other deployment models. [82]

Every deployment model except for public can allow the users of the cloud services to manage their own servers. This gives them control over the encryption of data and the keys to decrypt that data. However, many cloud services[83] depend on third party servers, wresting control away from the end user and allowing the cloud service provider to decide what data is encrypted and who has the capacity to decrypt that data.

B. LIMITED USE OF ENCRYPTION IN THE CLOUD

Unlike other contexts, the cloud has been slow to adopt encryption technologies. This may be because of the risks of encrypting data without a

76. Nat'l Inst. of Standards & Tech., *Final Version of NIST Cloud Computing Definition Published* (Oct. 25, 2011) (Press release), http://www.nist.gov/itl/csd/cloud-102511.cfm [https://perma.cc/3GLL-SM92].

77. Cindy Pham, *E-Discovery in the Cloud Era: What's a Litigant to Do?*, 5 HASTINGS SCI. & TECH. L.J. 139, 142 (2013).

78. *Id*. at 151.

79. *Id*. at 151-52.

80. *Id*. at 152-53.

81. *Id*. at 153.

82. *Id*. at 153-54.

83. For example: Gmail, Google Drive, Yahoo Mail, Apple iCloud, Dropbox, Amazon Web Services.

backup key. If a cloud provider encrypts data without any exceptional access protocol, there is a risk that a user could forget their password and leave everyone without access to the user's data. The value of access to data may also be limiting deployment. However, these concerns are counterbalanced by the growing cybersecurity threats to cloud service providers.

1. Cloud Business Models Disincentivize Encryption

Many cloud-based services, particularly those that offer free services, monetize user data.[84] That monetization requires that the companies have access to data that is stored on their servers, which may disincentivize the use of encryption.[85] This is evidenced by a July 2015 study by SkyHigh Networks.[86] The study analyzed 12,000 cloud providers and found that only 9.4% encrypted data at rest on their servers. Among those companies listed as storing data without encryption were Facebook, Twitter, LinkedIn, Gmail, PayPal, and eBay[87]—many companies that offer free services and largely drive their profits from monetization of data through targeted advertising.[88]

Another deterrent to utilization of encryption in the cloud is the difficulty that the creator of the data would face in searching and utilizing encrypted data. When data is encrypted, the difficulty of searching and indexing data is significantly increased.[89]

2. Security and Regulatory Incentives May Spur Deployment

There are, however, regulatory incentives for companies to encrypt the data they store on their servers. Data breaches have become a major

84. *See* Urs Gasser et al., *supra* note 6, at 10 ("For the past fifteen years, consumer-facing Internet companies have relied on advertising as their dominant business model. Ads are frequently used to subsidize free content and services. Internet companies more recently have been shifting towards data-driven advertising.").

85. *Id.* ("To fuel this lucrative market, companies typically wish to have unencumbered access to user data—with privacy assured through either restricting dissemination of identifiable customer information outside the boundaries of the company (and of governments, should they lawfully request the data). Implementing end-to-end encryption by default for all, or even most, user data streams would conflict with the advertising model and presumably curtail revenues.").

86. Cameron Coles, *Only 9.4% of Cloud Providers are Encrypting Data at Rest*, SKYHIGH NETWORKS (2015), https://www.skyhighnetworks.com/cloud-security-blog/only-9-4-of-cloud-providers-are-encrypting-data-at-rest/ [https://perma.cc/W9V8-9HQD].

87. *Id.*

88. *See* Urs Gasser et al., *supra* note 6, at 10.

89. *Id.* ("End-to-end encryption is currently impractical for companies who need to offer features in cloud services that require access to plaintext data.").

concern.[90] Recent breaches of private data, from companies both within and outside the tech industry, have led to the loss of private information of hundreds of millions of individuals.[91] From October 2014 to December 2015, there were eighty-three federal class action complaints resulting from data breaches.[92] In addition to the threats against privacy implicated by these breaches, there are significant monetary costs associated with a data breach. A study by IBM and the Ponemon Institute concluded that the average consolidated total cost of a data breach in the United States grew from $6,530,000 to $7,010,000 in 2016.[93] As data breaches continue to make headlines, companies may view encryption as a means to limit their risk, as thieves are less likely to try to steal encrypted data. Furthermore, even if encrypted data is stolen, the private information is more likely to remain secret.

Beyond the security benefits of encryption, regulations surrounding data breaches have begun to incentivize the use of encryption. Most states have specific data breach notification requirements, requiring notice to be sent to parties whose data may have been stolen in a data breach.[94] However,

90. *See* Privacy Rights Clearinghouse, *Chronology of Data Breaches: Security Breaches 2005–Present*, http://www.privacyrights.org/data-breach [https://perma.cc/9RLT-9VQV] (last visited Dec. 20, 2016) (showing 901,013,077 breached records from 5,245 data breaches made public since 2005).

91. *See e.g.,* Mark Fahey & Nicholas Wells, *Yahoo Data Breach is Among the Biggest in History*, CNBC (Sept. 22, 2016) (showing at least 500,000,000 breached accounts), http://www.cnbc.com/2016/09/22/yahoo-data-breach-is-among-the-biggest-in-history.html [https://perma.cc/H6HB-KSF3]; Off. of Personal Mgmt., *Cybersecurity Incidents* (showing two incidents with 21,500,000 breached social security numbers and 4,200,000 thefts of personal information on Federal government employees), https://www.opm.gov/cybersecurity/cybersecurity-incidents/ [http://perma.cc/73CZ-RXB5] (last visited Dec. 20, 2016); Jonathan Keane, *Security Researcher Dumps 427 Million Hacked Myspace Passwords Online*, DIGITAL TRENDS (July 1, 2016) (showing at least 427,000,000 breached accounts from Myspace data breach), http://www.digitaltrends.com/social-media/myspace-hack-password-dump/ [https://perma.cc/KKC2-R9QH].

92. BRYAN CAVE LLP, 2016 DATA BREACH LITIGATION REPORT 4 (2016), https://d11m3yrngt251b.cloudfront.net/images/content/8/2/v2/82494/DataBreachLitigationReport.pdf [https://perma.cc/88DP-SPS7].

93. PONEMON INSTITUTE, 2016 COST OF DATA BREACH STUDY: UNITED STATES 2 (2016), https://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03094usen/SEL03094USEN.PDF [https://perma.cc/6UJH-VPCA].

94. National Conference of State Legislatures, *Security Breach Notification Laws* (Jan. 4, 2016) ("Forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private, governmental or educational entities to notify individuals of security breaches of information involving personally identifiable information."), http://www.ncsl.org/research/telecommunications-and

almost all states and territories have encryption safe harbors.[95] Companies that know the stolen data was properly encrypted may therefore be exempt from the notice requirements.[96]

C. HEIGHTENED RISKS ON THE INTERNET

Data stored in the cloud is subject to a large number of security risks and attacks, as cloud systems are often highly interconnected and complicated.

1. Risks of External Attackers on a Large Attack Surface

Cloud providers face a significant challenge in protecting themselves against external threats. The more connected and complex a cloud service is, the more avenues there are for potential vulnerabilities to arise and be exploited. Security analysists refer to these avenues of attack as the "attack surface" of a given system.[97] Because cloud systems are constantly communicating with a large number of devices, storing and analyzing information on a variety of servers, and relying upon a large number of external devices and systems to perform analysis and data management, the "attack surface" of these systems can be vast. Because a potential vulnerability at *any* place in the system may compromise the system as a whole, cloud providers face an uphill battle in protecting complex networks from external threats.

2. Encryption Protects Against Some External Threats

Encryption does not necessarily reduce the surface area that attackers may exploit; nor does it prevent attacks from occurring. However,

---

-information-technology/security-breach-notification-laws.aspx [https://perma.cc/XE3D-Q9KB].

95. Baker & Hostetler LLP, *Data Breach Charts* (2016) (showing, as of January 1, 2017, that 49 states and territories grant some form of encryption safe harbor), https://www.bakerlaw.com/files/uploads/documents/data%20breach%20documents/data_breach_charts.pdf [http://perma.cc/YNS3-D5WF].

96. *See, e.g.,* 201 Mass. Code Regs. §§ 17.02(1)(a) (2009). Massachusetts defines a "breach of security" as: "[T]he unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information . . . that creates a substantial risk of identity theft or fraud against a resident of the Commonwealth."

97. . *See generally* TRIPWIRE, UNDERSTANDING YOUR ATTACK SURFACE: THE FIRST STEP IN RISK-BASED SECURITY INTELLIGENCE (2014) (discussing the three attack surfaces that organizations face: software attack surface, network attack surface, and human attack surface), http://www.tripwire.com/register/understanding-your-attack-surface-the-first-step-in-risk-based-security-intelligence/showMeta/2/ [http://perma.cc/UV4H-HHGD].

encrypting data stored in the cloud dramatically reduces the risks resulting from theft. An attacker who steals encrypted data would still need to find a way to decrypt the data, which may be impractical without access to the secret key used to encrypt the data.[98]

However, these benefits are not universal. There are methods whereby an attacker can gain access to unencrypted data even if the server stores data in an encrypted format. Data breaches involving misappropriation of data by insiders or social engineering would not necessarily be prevented even if data was encrypted. This is because insiders and employees have access to unencrypted data, which means they can provide that information to an outside attacker. In 2015, roughly 10% of all data breaches were a result of insider theft.[99]

3. Exceptional Access Erodes Security and Trust

Exceptional access to encryption in the cloud context undermines some of the protections that encryption provides. Because exceptional access would require that a key be stored in a manner accessible to the government, there is a risk that the key could also be accessible to an outside attacker.[100]

Regardless of the exact security risk that exceptional access would create, the mere threat of a vulnerability may have negative repercussions for trust in the cloud. If consumers and companies are aware of the security risks that exceptional access may implicate, consumers and companies may be less willing to store private information in the cloud.

Furthermore, this could also impact behaviors worldwide, as promulgating exceptional access would encourage authoritarian governments to demand access using the same methods the United States

98. VAUDENAY, *supra* note 8, at 21.

99. SYMANTEC, INTERNET SECURITY THREAT REPORT: VOLUME 21, 53 (2016), https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf [https://perma.cc/MSS4-DQWM].

100. *See* H Abelson et al., *supra* note 2, at 1, 12. The report states:

> [I]n a small but troubling number of cases, weakness related to [key escrow] requirements have emerged and been exploited by state actors and others. Those problems would have been worse had key escrow been widely deployed . . . the requirement of key escrow creates a long-term vulnerability: if any of the private escrowing keys are ever compromised, then all data that ever made use of the compromised key is permanently compromised. That is, in order to accommodate the need for surreptitious, third-party access by law enforcement agencies, messages will have to be left open to attack by anyone who can obtain a copy of one of the many copies of the law enforcement keys.

government would require.[101] This bears great risks to the protection of activists and journalists exposing human rights abuses, as their communications could be compromised.[102]

4. It Is Unclear if there Are Effective Alternatives to Encryption

If one operates under the assumption that exceptional access would undermine the security of encryption in the cloud, there are still some alternatives that may provide some (although not perfect) security. Systems that monitor traffic going in and out of servers, known as "intrusion detection systems," can watch for suspicious behavior and protect against external threats.[103] However, these systems will not be 100% effective at detecting malicious behavior and preventing attacks.[104]

D. LOW-TO-MEDIUM DISRUPTIVENESS

Based on these considerations, exceptional access in the cloud would likely have a low-to-medium disruptiveness impact. Encryption is one of the most effective solutions to minimize the impact of data breaches. However, encryption itself may stand at odds with the business interests of many cloud data providers, who want fast and efficient access to the data they store and monetize. At least for now, it appears that the interests of

---

101. *Id.* ("The US and UK governments have fought long and hard to keep the governance of the Internet open, in the face of demands from authoritarian countries that it be brought under state control. Does not the push for exceptional access represent a breathtaking policy reversal?").

102. *See* AMNESTY INTL., ENCRYPTION: A MATTER OF HUMAN RIGHTS 4 (2016) ("Encryption is a particularly critical tool for human rights defenders, activists and journalists, all of whom rely on it with increasing frequency to protect their security and that of others against unlawful surveillance"), http://www.amnestyusa.org/sites/default/files/encryption_-_a_matter_of_human_rights_-_pol_40-3682-2016.pdf [https://perma.cc/8V3Z-PGF6].

103. *See generally* NAT'L INST. OF STANDARDS AND TECH., NIST SPECIAL PUBLICATION 800-94, GUIDE TO INTRUSION DETECTION AND PREVENTION SYSTEMS (IDPS): RECOMMENDATIONS OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (2007). Likewise, other security measures, such as red-teaming or scanning e-mails for phishing attempts, can help protect organizations which store data remotely in the cloud.

104. *Id.* at § 2.3:

> Another common attribute of IDPS technologies is that they cannot provide completely accurate detection. When an IDPS incorrectly identifies benign activity as being malicious, a false positive has occurred. When an IDPS fails to identify malicious activity, a false negative has occurred. It is not possible to eliminate all false positives and negatives; in most cases, reducing the occurrences of one increases the occurrences of the other.

monetization are winning out over the interests of security in the cloud, as encryption is not widely deployed and data breaches are increasing in frequency and severity. Because of this, the disruptiveness of exceptional access to cloud-based data would be reduced. However, should encryption play a larger role in the security of the cloud in the future, mandating exceptional access would likewise become a more disruptive proposition.

IV. ENCRYPTION OF DATA IN-TRANSIT

Next, we can analyze the disruptiveness of exceptional access to data in-transit. Here, there is widespread use of encryption with increasing risks of attack, leading to a high level of disruptiveness.

A. TECHNOLOGY OF DATA IN-TRANSIT

In practice, the most common form of encryption of data in-transit uses Secure Sockets Layer and Transport Layer Security, commonly referred to as SSL/TLS.[105] SSL uses variations on the Diffie-Hellman key exchange protocol to provide both parties with a shared private key for communications.[106] This shared private key allows the communicating parties to establish an encrypted line of communication.[107] SSL also includes various protocols to ensure authentication through the use of certificates.[108] SSL is deployed in the HTTPS protocol, which websites can implement to encrypt data sent from their servers to internet browsers. [109]

B. WIDESPREAD USE ACROSS PLATFORMS

There are a large number of incentives for widely deployed encryption of data in-transit. Encryption allows for secure communications between

105. SCHMEH, *supra* note 14, at 343.

106. *Id.* at 346.

107. Companies are also beginning to integrate an innovation known as "forward secrecy" into their encryption schemes. This protocol allows for every single message sent between two parties to generate a unique, temporal, session key—meaning that a key is only applicable for the single message that it encrypted. Facebook has begun integrating forward secrecy into its messenger application, and WhatsApp already utilizes this protocol to encrypt communications between its users. *See* Scott Helme, *Perfect Forward Secrecy – An Introduction* (May 10, 2014), https://scotthelme.co.uk/perfect-forward-secrecy/ [https://perma.cc/G7A4-KTRF]; Andy Greenberg, *You Can All Finally Encrypt Facebook Messenger, So Do It* (Oct. 4, 2016), https://www.wired.com/2016/10/facebook-completely-encrypted-messenger-update-now/ [https://perma.cc/Z5MN-HD6P]; WhatsApp, *WhatsApp FAQ: End-to-End Encryption*, https://www.whatsapp.com/faq/en/general/28030015 [https://perma.cc/6VH5-MG25].

108. SCHMEH, *supra* note 14, at 354.

109. *Id.* at 353.

parties over the internet, which is important given the open structure of the internet.[110] Data exchanged between parties over the internet is routed through a wide array of devices and networks, potentially exposing data to a large number of prying eyes.[111]

In addition to the security benefits of encryption, there are regulations and standards that may require companies to implement encryption of data in-transit. The Gramm-Leach-Bliley Act imposes requirements for the banking and financial services industry to protect consumer data.[112] Companies under this regulatory umbrella are obligated to "respect the privacy" of their consumers and "protect the security and confidentiality of those consumers' non-public personal information"[113] Encryption can be a valuable tool for companies to ensure that customer data is private and secure.

Furthermore, regulatory agencies, such as the FTC, have used encryption as a metric in determining reasonable security standards. For example, in 2005 the FTC charged BJ's Wholesale with failing to provide reasonable security for sensitive customer information. Specifically, one of the allegations was that BJ's "failed to encrypt consumer information when it was transmitted . . . in BJ's stores."[114] In 2008, ValueClick was cited for "using only an insecure form of alphabetic substitution that [was] not consistent with, and less protective than, industry-standard encryption."[115] In 2016, the FTC settled with Henry Schein Practice Solutions, Inc. over

110. *Id.* at 20–21.

111. *Id.*

112. 15 U.S.C. § 6801(b) (1999). Which states, in part:

> [E]ach agency . . . shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards—
>
> (1) to insure the security and confidentiality of customer records and information;
>
> (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
>
> (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer. . . .

113. 15 U.S.C. § 6801(a) (1999) ("It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information . . . .").

114. Complaint at 2, *In Re BJ's Wholesale Club, Inc.*, No. 042 3160 (F.T.C. 2005).

115. Fed. Trade Comm'n, *ValueClick to Pay $2.9 Million to Settle FTC Charges* (2008) (Press release), https://www.ftc.gov/news-events/press-releases/2008/03/valueclick-pay-29-million-settle-ftc-charges [https://perma.cc/B47R-L6RF].

charges that the company falsely advertised the level of encryption provided to protect user data.[116] In fact, Terrell McSweeney, the FTC Commissioner, has gone as far as saying that: "I think mandating backdoors is a terrible idea." [117]

C. INCREASING RISKS WITH NO FEASIBLE ALTERNATIVE

Data in-transit is subject to interception, which encryption is designed to protect against. There are few robust alternatives to encryption which can provide security against the risk of interception.

1. Man-in-the-Middle Attacks Present a Risk to Data Security

Vulnerabilities in SSL/TLS encryption have shown their potential for harm. The "Heartbleed" vulnerability, for example, affected the OpenSSL implementation of SSL/TLS operating on web servers.[118] In response to this massive vulnerability, consumer trust may have been eroded in some online communications. A 2014 study by the Pew Research Center asked those familiar with the Heartbleed vulnerability about their responses to the attack. The study found that 39% of those polled took steps to secure their accounts and information by doing such things as changing passwords or canceling accounts, and 29% of those polled believed their personal information was put at risk because of Heartbleed.[119]

2. Encryption Is Effective at Mitigating Risks

Encryption, when properly implemented, is effective at protecting against man-in-the-middle attacks. When data is encrypted, the content of that data is unreadable to any eavesdroppers, preserving the confidentiality of the communications. If lengthy session keys are kept secret and the encryption algorithm is sufficiently robust, it is computationally infeasible for an attacker to obtain any plaintext from encrypted data in-transit.[120]

---

116. Fed. Trade Comm'n, *Dental Practice Software Provider Settles FTC Charges It Misled Customers About Encryption of Patient Data* (2016) (Press release) https://www.ftc.gov/news-events/press-releases/2016/01/dental-practice-software-provider-settles-ftc-charges-it-misled [https://perma.cc/JB4B-VN9Z]

117. Eric Geller, *FTC commissioner: Mandating encryption backdoors 'is a terrible idea,'* DAILY DOT (May 24, 2016).

118. *See generally* Zakir Durumeric et al., *The Matter of Heartbleed,* PROCEEDINGS OF THE 2014 CONFERENCE ON INTERNET MEASUREMENT 475–88 (Nov. 2014).

119. PEW RESEARCH CENTER, HEARTBLEED'S IMPACT 3 (Apr. 2014), http://www.pewinternet.org/files/2014/04/PIP_Heartbleed-impact_043014.pdf [https://perma.cc/J3GD-46SK].

120. VAUDENAY, *supra* note 8, at 21.

3. Exceptional Access Could Undermine Encryption's Effectiveness and Hamper Innovation

Mandating exceptional access for existing technologies such as SSL/TLS would require fundamental changes to the technology underlying encryption of data in-transit. Key exchange protocols are designed to protect the confidentiality of secret session keys used to encrypt data during communications. If the protocol must allow for exceptional access, there either must be a vulnerability in the key exchange protocol, which could allow an attacker to gain access to the secret session key, or there must be a "master key" which allows decryption regardless of the specific session key. Either requirement would fundamentally undermine the security of the existing SSL/TLS framework.

Beyond the technical risks associated with exceptional access to data in-transit, there is a potential for a chilling effect on the public's trust in secure communication channels. The already limited trust in the security of online communications[121] could be further eroded if consumers knew that security vulnerabilities are integrated into the encryption protocols. Furthermore, the concerns about human rights abuses and authoritarian governments expressed above in Section III.C.3 are also relevant to exceptional access to data in-transit. A requirement for exceptional access may also limit technical innovation on encryption of data in-transit. Innovations such as forward secrecy[122] are at odds with exceptional access to data in-transit.

4. No Feasible Alternative Currently Exists

Man-in-the-middle attacks are difficult to detect in the absence of SSL/TLS encryption. The creation of a vulnerability in SSL may discourage its use generally, which may harm some of the authentication benefits SSL provides. Many current attack detection schemes rely upon finding spoofed

121. *See* PEW RESEARCH CENTER, PUBLIC PERCEPTIONS OF PRIVACY AND SECURITY IN THE POST-SNOWDEN ERA 4 (Nov. 2014) (showing that 81% feel "not very" or "not at all secure" using social media sites when they want to share private information with another trusted person or organization, 68% feel insecure using chat or instant messages to share private information, and 57% feel insecure sending private information via email), http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf [https://perma.cc/CG6M-4HCV].

122. Exceptional access requires that *all* messages be available. Either every single message's session key would need to be accessible or a "master key" would need to be able to access every single message, defeating the purpose of forward secrecy should the master key become stolen.

SSL certificates (used for authentication),[123] which is impracticable if SSL is not utilized due to concerns with confidentiality.

D. HIGH DISRUPTIVENESS

Given the great number of risks associated with mandating exceptional access to data in-transit, it appears likely that a mandate would be a highly disruptive proposition. Exceptional access could undermine the security of financial transactions, VPNs, remote management of critical infrastructure systems, personal communications, health communications, and login information. Consumer trust may (rightfully) erode in these communications, hampering progress in utilizing the internet to help consumers manage their financial accounts, health data, and more. Furthermore, this type of encryption is widely adopted and there is no feasible alternative for protecting user data online.

Finally, a mandate of exceptional access doesn't square with prevailing regulatory movements toward encryption. As agencies like the FTC push companies to better secure data and implement encryption-based security practices, exceptional access gives rise to new risks that these security practices are vulnerable to attack.

V. ENCRYPTION OF ENDPOINTS

Finally, we can turn to the disruptiveness of exceptional access to endpoint devices. Here, there is currently limited use of encryption and there are a number of alternatives which may adequately protect data stored on endpoint devices, leading to medium disruptiveness.

A. TECHNOLOGY OF ENDPOINT ENCRYPTION

Data at endpoints can be encrypted at the device level or the file level. The manner in which data is encrypted can affect the strength of that encryption and limit brute-force attacks.

1. Encryption of Devices vs. Files

Endpoint encryption can be implemented to encrypt the entirety of a hard disk (full disk encryption), or to apply to individual files or folders

123. *See, e.g.,* Lin-Shung Huang et al., *Analyzing Forged SSL Certificates in the Wild*, PROC. OF THE 2014 IEEE SYMP. ON SECURITY AND PRIVACY 83–97 (2014); Peter Burkholder, *SSL Man-in-the-Middle Attacks*, SANS INST. INFOSEC READING ROOM (2002).

within a hard disk (partial disk encryption).[124] While the underlying principles for encryption are the same no matter what content is encrypted, each of these implementations involves a different method of utilizing encryption, leading to differing approaches required for exceptional access.

Full disk encryption may be applied when a device is locked or powered down or may operate in real time as the device is being used.[125] When the device is encrypted when locked, a hardware mechanism can be used to encrypt the drive and subsequently decrypt the drive when the proper password is provided on boot.[126] An alternative solution is software encryption, where the device, either on lock or on boot, runs a program that allows for data on the device to be encrypted/decrypted.[127] Partial disk encryption is typically accomplished with software that runs on the device, encrypting or decrypting the files provided to it.[128]

2. Limiting Effectiveness of Brute-Force Attacks

Hardware-based implementations are advantageous because they can be integrated into the device itself and configured to make brute-force attacks impracticable. This prevents a situation where an attacker extracts the data from the device onto a more powerful computer in order to try to crack the encryption more quickly.[129]

For example, newer versions of the iPhone contain an integrated cryptographic processor called a "Secure Enclave."[130] This crypto processor contains a unique number tied to the specific device known as a "unique

124. NAT'L INST. OF STANDARDS AND TECH., NIST SPECIAL PUBLICATION 800-111, GUIDE TO STORAGE ENCRYPTION TECHNOLOGIES FOR END USER DEVICES 5–9 (2007).

125. *Id.* at 5.

126. *Id.*

127. *Id.* at 8.

128. *Id.* at 9.

129. Dedicated hardware for brute-force attacks can drastically increase the speed of an offline brute-force attack. For example, a dedicated brute force system used at the Passwords^12 Conference in Oslo, Norway was able to guess 348 billion hashed passwords using the popular NTLM algorithm. Practically, this means that it could guess any eight-character password in five and a half hours—assuming there is no hardware preventing brute force guessing. Paul Roberts, *Update: New 25 GPU Monster Devours Passwords in Seconds*, SECURITY LEDGER (Dec. 4, 2012), https://securityledger.com/2012/12/new-25-gpu-monster-devours-passwords-in-seconds/ [https://perma.cc/E9SX-XFE6].

130. Apple, *iOS Security Guide: iOS 9.3 or Later* (May 2016); Mike Ash, *What is the Secure Enclave?* (Feb. 19, 2016) https://www.mikeash.com/pyblog/friday-qa-2016-02-19-what-is-the-secure-enclave.html [https://perma.cc/QK4H-T2RZ]; *See generally* Tarjei Mandt, *Demystifying the Secure Enclave Processor* (presentation from Black Hat USA 2016), https://www.blackhat.com/docs/us-16/materials/us-16-Mandt-Demystifying-The-Secure-Enclave-Processor.pdf [https://perma.cc/72JD-UX84].

identifier" (UID).[131] This UID is then combined with the user's password to provide the encryption key used to encrypt or decrypt the iPhone's data.[132] The UID is not accessible outside of the Secure Enclave, meaning that any attempt to derive the encryption key must be done through the Secure Enclave.[133] Because all password guess attempts must go through the Secure Enclave, Apple was able to integrate various delay functions into the Secure Enclave after successive incorrect guesses[134] and can wipe the phone after a certain point.[135]

B. LIMITED USAGE WITH POTENTIAL FOR GROWTH

While encryption is currently underutilized on endpoint devices, new innovations are bringing encryption to the masses.

1. Consumer Device Manufacturers Are Making Encryption Accessible

Companies have responded to the increased demand for privacy by making device-level encryption accessible to virtually anyone. Both iPhones[136] and Android[137] phones allow users to integrate encryption into the existing password protections on their devices. Microsoft[138] and Apple[139] have also integrated device encryption into certain versions of their Windows and OS X computer operating systems. In addition to the full disk encryption offered by major software and hardware developers, a number of programs allow users to easily encrypt specific files and folders on their devices.[140]

131. Mike Ash, *What is the Secure Enclave?* (Feb. 19, 2016), https://www.mikeash.com/pyblog/friday-qa-2016-02-19-what-is-the-secure-enclave.html [https://perma.cc/QK4H-T2RZ].

132. *Id.*

133. *Id.*

134. *Id.*

135. *Id.*

136. Apple, *iOS Security Guide: iOS 9.3 or Later* (May 2016).

137. Android, *Encryption*, https://source.android.com/security/encryption/ [https://perma.cc/9SSB-QY3S].

138. Microsoft, *BitLocker Drive Encryption Overview* (2016), https://technet.microsoft.com/en-us/library/cc732774.aspx [https://perma.cc/ZT7R-VKYR].

139. Apple, *Use FileVault to Encrypt the Startup Disk on Your Mac* (Dec. 2016), https://support.apple.com/en-us/HT204837 [https://perma.cc/FZ9N-EP9C].

140. For example, free software like AxCrypt can encrypt specific files or folders with user chosen passwords.

2. *Despite Access, Many Endpoint Devices Are Still Not Protected by Encryption*

For consumers, a 2014 study by Consumer Reports found that only 47% of smartphone users actually set a screen lock with a PIN, password, or unlock pattern.[141] If users fail to implement encryption on their devices, the presence of exceptional access makes little difference.

The enterprise also shows low usage of encryption. A 2015 survey of 1,700 IT decision makers around the world suggested that only 60% of organizations encrypted their laptops with encryption and only 29% of organizations encrypted their smartphones or tablets.[142] However, encryption may become more widespread, as 90% of organizations reported planning to extend their data protection approach with encryption,[143] and 69% were planning to do so within the next one to two years.[144]

C. ALTERNATIVE SOLUTIONS CAN TEMPER EXCEPTIONAL ACCESS RISKS

Encryption may not be the only method to ensure that data is kept safe on lost or stolen endpoint devices, and alternative solutions may limit some of the risks of mandating exceptional access.

1. *Lost or Stolen Devices Represent a Serious Risk*

In 2013, 1.4 million smartphones were lost and 3.1 million stolen,[145] so a policy requiring exceptional access could have far-reaching consequences to the security of consumer data. While exceptional access schemes may be designed to minimize the risk of a "master key" being released or to complicate the task of circumventing encryption, there is virtually no way to ensure that exceptional access would only apply to the proper parties and

141. Consumer Reports, *Smart Phone Thefts Rose to 3.1 Million in 2013* (May 2014) (36% used a 4-digit PIN while 11% used a PIN longer than 4 digits, a password, or unlock pattern), http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm [https://perma.cc/67D4-S4TU].

142. SOPHOS, THE STATE OF ENCRYPTION TODAY: RESULTS OF AN INDEPENDENT SURVEY OF 1700 IT MANAGERS 5 (Dec. 2015), https://secure2.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/the-state-of-encryption-today-wpna.pdf?la=en [https://perma.cc/LB9U-SBZG].

143. It is not completely clear whether this refers to encryption of data at endpoints, data in the cloud, or data in-transit; however, this still suggests that encryption (as a whole) will become more widespread in the coming years.

144. SOPHOS, *supra* note 142, at 9.

145. Consumer Reports, *supra* note 141.

would never be inappropriately used by third parties.[146] This risk may cause consumer trust in their devices to erode.

2. Encryption Can Minimize This Risk

Device-level encryption blocks access to all data on a device unless the user enters a password. In addition to protecting data, this powerful security may deter the theft of devices. If an adversary knows that a device will be locked and inaccessible, there is very little to gain from stealing that device. As a result, widely deployed encryption may reduce the prevalence of device theft.

3. Exceptional Access Can Undermine Security and Chill Usage

Because endpoint encryption primarily serves to protect against lost or stolen devices, exceptional access may limit the security of data on lost or stolen devices. Exceptional access, whether that be through some sort of "master key" or a method to circumvent the encryption protections on a device, could allow a thief to gain access to the very data that is supposed to be secure.

Seminal privacy cases, such as *Riley v. California*, and the arguments of *Amici* in the San Bernardino litigation exemplify the concerns over exceptional access. As the court in *Riley* noted, "Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'"[147] The protection of the content of electronic devices (whether encrypted or not) has been recognized in American jurisprudence apart from *Riley*.[148]

Likewise, the *amici* for Apple in the San Bernardino case argued that exceptional access may "forever alter" the relationship between technology providers and users, as these "vulnerabilities could be exploited to the

146. *See* H Abelson et al., *supra* note 2, at 7 ("An organization that holds an escrow key could have a malicious insider that abuses its power or leaks that organization's key. Even assuming an honest agency, there is an issue of competence: cyberattacks on keyholders could easily result in catastrophic loss."). The additional complexity of a key escrow system compounds these risks.

147. *Riley v. California*, 134 S. Ct. 2473 (2014) (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)).

148. *See e.g.*, *United States v. Doe*, 670 F.3d 1335 (11th Cir. 2012) (holding that compelled decryption of an encrypted hard drive would violate the 5th Amendment); *United States v. Graham*, 796 F.3d 332 (4th Cir. 2015) (holding that the government engages in a Fourth Amendment search when it examines historical cell site location information stored on a cell phone); *United States v. Whiteside*, 2015 U.S. Dist. LEXIS 84369 (S.D.N.Y. 2015) (extending the protections of *Riley* to digital cameras).

detriment of everyone who uses connected devices."[149] There is a risk that exceptional access may have chilling effects on how people treat data. Users may be reluctant to store personal information on devices they feel are insecure.

4. Alternatives to Encryption Also Mitigate Some Risks

While encryption is a powerful tool for protecting endpoint devices, it is far from the only method of ensuring that data on devices remain secure. For example, "Find My iPhone"[150] or "Android Device Manager"[151] allow users to remotely find, lock, and wipe devices connected to the internet. In addition, these systems are based on the user's Apple ID or Google Account, which is accessible to the manufacturers of the devices (and therefore to the government with legal authority). However, because these non-encryption systems require that a device be connected to the internet to function effectively, these alternatives are not a complete replacement to the security benefits that encryption offers to endpoint devices.

D. MEDIUM DISRUPTIVENESS

All-in-all, exceptional access to endpoint devices likely comes out around the middle of the disruptiveness scale. Regardless of the exact extent to which exceptional access may create new vulnerabilities and the extent to which those vulnerabilities are actively exploited, there are undoubtedly risks associated with mandating exceptional access to endpoint devices. Exceptional access creates new vulnerabilities in encryption, harming both cybersecurity and the public's perception of the security of their devices. There is potential for data theft arising from lost or stolen devices to increase

149. Brief of the Center for Democracy & Technology as *Amicus Curiae* in Support of Apple Inc.'s Motion to Vacate and in Opposition to Government's Motion to Compel Assistance at 6-7, *In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203* (2016) (ED No. CM 16-10 (SP)); *see also* Brief of *Amicus Curiae* AirBnB, Inc., *supra* note 59, at 4 ("ensuring that users' data is handled in a safe, secure, and transparent manner that protect privacy is of utmost importance."); Brief of *Amici Curiae* Amazon.com, Box, Cisco Systems, Dropbox, Evernote, Facebook, Google, Microsoft, Mozilla, Nest, Pinterest, Slack, Snapchat, Whatsapp, and Yahoo in Support of Apple, Inc. at 18, *In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203* (2016) (ED No. CM 16-10 (SP)) ("[A]s storing sensitive personal and commercial data electronically becomes less of a luxury and more of a necessity, protecting that data has also become a necessity.").

150. Apple, *Find My iPhone, iPad, and Mac*, http://www.apple.com/icloud/find-my-iphone.html [https://perma.cc/VV8R-BPXY].

151. Google, *Find Your Device Using Android Device Manager*, https://support.google.com/accounts/answer/6160491 [https://perma.cc/6Q5W-V82J].

as even encrypted data may be accessible via vulnerabilities that exceptional access introduces.

On the other hand, the lack of utilization of encryption and the existence of alternatives to encryption helps counterbalance the risks of exceptional access. Many of the risks that encryption protects against may be mitigated using methods that don't impede government access to data. Today, encryption is easier to deploy than ever before, however consumers and the enterprise are still not utilizing encryption en masse. Some may see this as a sign that consumers and the enterprise feel that non-encryption based security methods are sufficient and better align with their goals, such as having access to employee data and not getting locked out of their own devices.

VI. WHERE DO WE GO FROM HERE?

The limited analysis provided is an example of how the framework can be used. Substantially more in-depth consideration of the disruptiveness factors would be required to fully understand the complete disruptiveness that could arise from exceptional access in each of these contexts.

Given the contentious nature of the debate over encryption, reaching consensus on exceptional access is an uphill battle. Fundamental disagreements in worldview and culture put technologists at odds with the government; however, public opinion may force policymakers into making decisions that one (or both sides) may not love, but nevertheless would have to live with.

For the discussion to move forward, trying to compare these risks in the framework of disruptiveness can give a sense of where progress may be possible and where the risks are just too high. Above all else, a nuanced and technically-minded discussion of the issues is the only way to ensure that encryption policy thoughtfully assesses risks and balances the goals of our country—from cybersecurity to national security.