VIRGINIA LAW REVIEW ONLINE

VOLUME 110 MARCH 2024 70–88

ESSAY

20/20 HINDSIGHT AND LOOKING AHEAD: THE VISION OF THE FIVE EYES AND WHAT'S NEXT IN THE "GOING DARK" DEBATE

*Hayley S. Brower & Daniel S. McCray**

The so-called "encryption debate" made national headlines in 2016 after Apple Inc. ("Apple") declined to enable the Federal Bureau of Investigation ("FBI" or "the Bureau") to unlock an iPhone recovered from one of the shooters involved in a terrorist attack in San Bernardino, California. The debate concerned whether the government should have the authority to compel technology manufacturers to create an "access key" for encrypted messages and share that key with law enforcement. Apple argued that allowing such access would undermine the security features of its products, while the U.S. Department of Justice ("DOJ") insisted access was necessary to prevent future attacks. An existing dilemma came to the forefront: Should technology companies be able to use forms of encryption so secure that even they lack the keys? Or is such security not worth the possibility of allowing criminals to "go dark" from law enforcement?

While public attention on this issue has waned in recent years, the problem is not going away; instead, answers are needed now more than ever. As recently as December 2023, a leading technology company

* J.D. Candidates, University of Virginia School of Law (expected 2024). We are grateful to Dennis Ting, Heream Yang, and the editors of the *Virginia Law Review* who brought this Essay to publication.

announced it would use end-to-end encryption ("E2EE") as a default for calls and messages across some of its platforms. Analyzing the strengths and weaknesses of laws passed in other countries in The Five Eyes provides guidance for how the U.S. may best proceed with future legislation to promote privacy and security on a global scale.

INTRODUCTION

In 2015, then-FBI Director James Comey testified before the Senate Judiciary Committee, saying, "There's no doubt that [the] use of encryption is part of terrorist tradecraft now."[1] Months earlier, a heavily armed couple had killed fourteen people and seriously injured seventeen others in San Bernardino, California.[2] As part of its investigation, the Bureau obtained a warrant to search an iPhone owned by one of the shooters, but the phone was programmed to automatically delete all data after ten failed password attempts.[3] Unable to unlock the phone due, in part, to encrypted user data, the FBI requested that Apple rewrite its software to disable security features and install it for investigators to gain access.[4] Apple refused, arguing that deliberately weakening encryption on its devices by creating a "backdoor" through the encryption for law enforcement would make its products more susceptible to hacking by bad actors and foreign governments.[5]

[1] Sen. Charles E. Grassley Holds a Hearing on Oversight of the Federal Bureau of Investigation, S. Comm. on Judiciary (Dec. 9, 2015), https://congressional.proquest.com/congressional/docview/t65.d40.12090003.s98?accountid=14678 [https://perma.cc/DR82-DBN3].

[2] Adam Nagourney, Ian Lovett & Richard Pérez-Peña, San Bernardino Shooting Kills at Least 14; Two Suspects Are Dead, N.Y. Times (Dec. 2, 2015), https://www.nytimes.com/2015/12/03/us/san-bernardino-shooting.html [https://perma.cc/4UJN-B78T].

[3] Daniel Kahn Gillmor, One of the FBI's Major Claims in the iPhone Case is Fraudulent, ACLU (Mar. 7, 2016), https://www.aclu.org/news/privacy-technology/one-fbis-major-claims-iphone-case-fraudulent [https://perma.cc/YYF5-8UMQ].

[4] Government's Ex Parte Application for Order Compelling Apple Inc. to Assist Agents in Search 1–2; Memorandum of Points and Authorities at 1–2, 4, 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. 15-mj-00451 (C.D. Cal. Feb. 16, 2016).

[5] See Letter from Tim Cook, CEO of Apple, to Apple Customers (Feb. 16, 2016), https://www.apple.com/customer-letter/ [https://perma.cc/P5G9-5A7N]; Apple's Tim Cook: Complying with FBI Demand "Bad for America," CBS News (Feb. 24, 2016, 9:02 PM), https://www.cbsnews.com/news/apples-tim-cook-complying-with-fbi-demand-bad-for-america/ [https://perma.cc/59FU-YKXR]; Shara Tibken, Countdown to Doomsday: Apple, FBI Face Off in Court Tuesday, CNET (Mar. 19, 2016, 5:00 AM), https://www.cnet.com/news/privacy/apple-fbi-case-encryption-iphone-backdoor-hack-terrorism-privacy-surveillance/ [https://perma.cc/5AFT-H2LW].

The dispute between Apple and the DOJ is the most prominent example of an ongoing and contentious debate about government regulation of E2EE.[6] E2EE describes a secure communication method that prevents third-party access to data transferred from one device to another.[7] Many forms of encryption can be accessed by anyone with the appropriate decryption key, but E2EE goes beyond other forms of encryption by limiting access to messages and data to only the communicating parties.[8] E2EE scrambles data so only the sender and intended recipient may read E2EE messages; not even the manufacturer of the communication devices can access such data.[9] E2EE also ensures that data is encrypted before it is sent over a network, avoiding exposure of such communications to bad actors (such as hackers) in the event of a data breach.[10] In this way, E2EE is considered the gold standard for ensuring consumer privacy. However, E2EE's airtight seal means law enforcement may not be able to effectively investigate dangerous criminal activity unless the encryption is weakened. The modern encryption debate centers around a challenging dilemma: Should the government be able to compel technology companies to build systems in such a way that permits law enforcement access? Or should considerations about safeguarding privacy be paramount, even at the expense of governmental investigation and oversight?

Over the years, the two sides of the conversation have become increasingly polarized, with law enforcement groups on one side and privacy and civil liberties advocates on the other. Much has been written about the constitutionality of potential solutions to the cryptology debate. This Essay adds a new, unique perspective to the existing literature by discussing it within the context of rapidly evolving technology making E2EE policies instrumental to the lives of most Americans. Part I provides

[6] See Reema Shah, Comment, Law Enforcement and Data Privacy: A Forward-Looking Approach, 125 Yale L.J. 543, 543 (2015).

[7] Mallory Knodel, Fred Baker, Olaf Kolkman, Sofía Celi & Gurshabad Grover, Definition of End-to-End Encryption, Internet Eng'g Task Force (June 13, 2022), https://www.ietf.org/archive/id/draft-knodel-e2ee-definition-04.html [https://perma.cc/8W7P-FG5L].

[8] Steven Song, Keeping Private Messages Private: End-to-End Encryption on Social Media, B.C. Intell. Prop. & Tech. F., 2020, at 1, 2.

[9] How End-to-End Encryption in Google Messages Provides More Security, Google Messages, https://support.google.com/messages/answer/10262381?hl=en [https://perma.cc/2H7S-R3GX] (last visited Feb. 25, 2024).

[10] Lucian Armasu, End-to-End Encryption Could've Protected Yahoo Mail Users from 2014 Data Breach and NSA Spying, Tom's Hardware (Oct. 14, 2016), https://www.tomshardware.com/news/e2ee-yahoo-mail-hack-spying,32857.html [https://perma.cc/YGQ7-K5G2].

an overview of the debate within the technology and law enforcement communities and describes the failures of Congress to address the issue. Part II evaluates the strength of Australia's and the United Kingdom's approaches for addressing the problem. Finally, Part III provides recommendations for what Congress should do to address the encryption debate.

I. THE E2EE DEBATE: LAW ENFORCEMENT AND THE TECHNOLOGY SECTOR CONTINUE TO DISAGREE WHILE CONGRESS FAILS TO ACT

A. The Tension Between Law Enforcement Needs and Privacy Advocates' Security Concerns

The E2EE debate has pitted law enforcement groups and privacy advocates against each other. Many privacy advocates have argued that enhanced consumer security and privacy enabled by E2EE should be preserved to the fullest.[11] Meanwhile, some law enforcement groups have maintained that such "warrant-proof" encryption inhibits law enforcement's investigative capabilities by preventing access to certain information otherwise authorized by a search warrant or wiretap order.[12]

To intercept serious crimes, law enforcement agencies and prominent government officials argue that communications providers should include "backdoors" in their E2EE technology so law enforcement can access otherwise encrypted messages.[13] Former U.S. Attorney General William Barr, joined by officials in the U.K. and Australia, sent a letter to Meta founder Mark Zuckerberg urging Facebook (now Meta) "not [to] proceed with its plan to implement end-to-end encryption across its messaging services without . . . including a means for lawful access to the content of

[11] See, e.g., Paul McLaughlin, Crypto Wars 2.0: Why Listening to Apple on Encryption Will Make America More Secure, 30 Temp. Int'l & Compar. L.J. 353, 355 (2016); Harold Abelson et al., Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications, 1 J. Cybersecurity 69, 78 (2015); Eric Manpearl, The International Front of the Going Dark Debate, 22 Va. J.L. & Tech. 158, 167 (2019).

[12] See, e.g., The Lawful Access Challenge, Fed. Bureau of Investigation, https://www.fbi.gov/about/mission/lawful-access [https://perma.cc/7UBG-6QGM] (last visited Feb. 25, 2024); Critical Issues: Encryption & Going Dark, Int'l Ass'n of Chiefs of Police, https://www.theiacp.org/resources/critical-issues-encryption-going-dark [https://perma.cc/QZ8Y-ZV7B] (last visited Feb. 25, 2024).

[13] Pragya Jain, Encryption: A Tradeoff Between User Privacy and National Security, Am. Univ. (July 15, 2021) https://www.american.edu/sis/centers/security-technology/encryption.cfm [https://perma.cc/APP2-QG5C].

communications to protect our citizens."[14] Former Deputy Attorney General Rod Rosenstein also called upon technology experts to look for ways to create feasible "backdoor" technologies despite the fact that "[s]ome technology experts castigate colleagues who engage with law enforcement to address encryption and similar challenges."[15]

On the other side of the debate, privacy advocates argue the government has not shown a real need for exceptional access. They claim the government already has extensive investigative tools[16] to collect all the information it needs.[17] Additionally, technology companies have expressed serious doubts regarding the technological feasibility of providing law enforcement with exceptional access via encryption keys without also seriously compromising consumers' security.[18] They further argue that providing exceptional access circumvents the "best practices now being deployed to make the Internet more secure."[19] As a result, technology companies have moved away from retaining encryption keys to better secure consumers' communications.[20] They also argue that communication systems would become detrimentally complex if service providers were required to implement exceptional access for law enforcement because "every new feature can interact with others to create

[14] Open Letter from Rt. Hon. Priti Patel, U.K. Sec'y of State for Home Dep't, William P. Barr, U.S. Att'y Gen., Kevin K. McAleenan, U.S. Sec'y of Homeland Sec. (Acting) & Hon. Peter Dutton, Australian Minister for Home Affs., to Mark Zuckerberg, Chief Exec. Officer, Facebook (Oct. 4, 2019), https://www.justice.gov/d9/press-releases/attachments/2019/10/03/open_letter_to_mark_zuckerberg.final_0.pdf [https://perma.cc/WGQ5-5A63]; see also Sean Gallagher, Barr Says the U.S. Needs Encryption Backdoors to Prevent "Going Dark." Um, What?, Ars Technica (Aug. 4, 2019, 9:30 AM), https://arstechnica.com/tech-policy/2019/08/post-snowden-tech-became-more-secure-but-is-govt-really-at-risk-of-going-dark/ [https://perma.cc/PA8E-GFK9] (quoting Attorney General Barr, who remarked that end-to-end encryption allows "criminals to operate with impunity").

[15] Lily Hay Newman, Deputy AG Rod Rosenstein is Still Calling for an Encryption Backdoor, Wired (Nov. 29, 2018, 6:01 PM), https://www.wired.com/story/rod-rosenstein-encryption-backdoor/ [https://perma.cc/F5Y6-SAYA] (explaining that Deputy Attorney General Rod Rosenstein stated that "[t]here is nothing virtuous about refusing to help develop responsible encryption").

[16] Some examples of the tools used by law enforcement are "vulnerability-based unlocking toolkits" and obtaining back-up copies of the data which can later be decrypted. Carl Landwehr, Privacy and Security: Encryption and Surveillance, 62 Viewpoints 27, 28 (2019).

[17] Id.

[18] Id.; Jain, supra note 13.

[19] See Abelson et al., supra note 11, at 70.

[20] Jennifer Stisa Granick & Daniel Kahn Gillmor, The Vital Role of End-to-End Encryption, ACLU (Oct. 20, 2023), https://www.aclu.org/news/privacy-technology/the-vital-role-of-end-to-end-encryption [https://perma.cc/JA4P-7UYW].

vulnerabilities."[21] Finally, technology companies insist that allowing exceptional access provides an opportunity for hackers and other bad actors to gain access to the encryption key information.[22]

While many technology experts share the industry's views, the validity of an "encryption at all costs" position has been debated. For instance, Ray Ozzie, the former chief technical officer and former chief software architect of Microsoft Corporation, has stated that if vendors of communication technology can be trusted with updating users' devices, then the "user should be able to trust the vendor to manage keys that can provide exceptional access."[23] According to Ozzie, "In engineering[,] if you think hard enough, you can come up with a solution."[24] Still others have contended that, even if exceptional access is deemed undesirable, alternative strategies may provide a "middle-ground" of sorts. Some advocate for a deeper look into "lawful hacking" strategies, which would allow law enforcement to hack computers without using decryption keys.[25]

B. Congress's Attempts and Failures in Passing E2EE Legislation

Shortly after the San Bernardino attack, former Senators Richard Burr (R-NC) and Dianne Feinstein (D-CA) introduced the Compliance with Court Order Act ("CCOA"), which aimed to provide law enforcement with the authority to compel technology companies to grant government access to encrypted messages.[26] The bill was specifically intended to ensure criminals and terrorists could not rely on encryption to conceal

[21] Abelson et al., supra note 11, at 70; see also Stefan Soesanto, No Middle Ground: Moving on From the Crypto Wars, Eur. Council on Foreign Rels. (July 5, 2018), https://ecfr.eu/publication/no_middle_ground_moving_on_from_the_crypto_wars [https://perma.cc/8Q8R-24HP] (arguing that there is no middle ground which would feasibly allow responsible encryption to be implemented).

[22] Abelson et al., supra note 11, at 70.

[23] Nat'l Acads. Scis., Eng'g & Med., Decrypting the Encryption Debate: A Framework for Decision Makers 57 (2018).

[24] Steven Levy, Cracking the Crypto War, Wired (Apr. 25, 2018, 6:00 AM), https://www.wired.com/story/crypto-war-clear-encryption/ [https://perma.cc/6TBK-3C9E].

[25] Nat'l Acads. Scis., Eng'g & Med., supra note 23, at 55 ("For example, the government may obtain a warrant to secretly insert software on a targeted computer that surreptitiously records every keystroke on a computer. This can be used to capture the suspect's passwords, thus allowing access to everything else.").

[26] Compliance with Court Orders Act of 2016, 114th Cong. (2016) (Discussion Draft), https://web.archive.org/web/20160413195503/https://www.burr.senate.gov/imo/media/doc/BAG16460.pdf [https://perma.cc/7E6T-NRJP].

illegal activities.[27] Senator Feinstein stated: "We need strong encryption to protect personal data, but we also need to know when terrorists are plotting to kill Americans."[28] In addition to assisting efforts to combat terrorism, supporters also argued the bill was necessary to stop other serious crimes, including the dissemination of child pornography, illicit drug trades, and human trafficking efforts.[29]

The bill's language required that, upon the receipt of a court order or warrant, specified entities must provide the government with data in its "intelligible" (unencrypted) form or provide law enforcement entities with technical assistance necessary to render the data intelligible.[30] A covered entity[31] would be required to provide data in an intelligible format "if such data has been made unintelligible by a feature, product, or service owned, controlled, created, or provided, by the covered entity" or a third party on that entity's behalf.[32] The technical assistance would include the entity "isolating" the device's information or data, decrypting it, and delivering the information or data to the requesting agency.[33] The bill also allowed for compensation to be provided to covered entities for costs "reasonably necessary and which have been directly incurred in providing such technical assistance."[34]

[27] See id. § 2(4)–(5); Feinstein's Anti-Encryption Bill Provokes Fear in Silicon Valley Tech Firms, CBS News (Apr. 21, 2016, 6:40 PM), https://www.cbsnews.com/sanfrancisco/news/feinsteins-anti-encryption-bill-provokes-fear-in-silicon-valley-tech-firms [https://perma.cc/4LE5-B57N].

[28] Feinstein's Anti-Encryption Bill Provokes Fear in Silicon Valley Tech Firms, supra note 27.

[29] See Feinstein Bill Would Require Social Media Companies to Report Online "Terrorist Activity," CBS News (Dec. 8, 2015, 2:42 PM), https://www.cbsnews.com/losangeles/news/feinstein-bill-would-require-social-media-companies-to-report-online-terrorist-activity/ [https://perma.cc/6VCB-4Q7T]; Counterterrorism, Counterintelligence, and the Challenges of "Going Dark": Hearing Before the Select Comm. on Intel. of the U.S. Senate, 114th Cong. 2 (2015), https://www.intelligence.senate.gov/sites/default/files/hearings/S.%20Hrg.%20114-739.pdf [https://perma.cc/H96A-TVLR] (statement of Sen. Richard Burr, Chairman, Select Comm. on Intel.).

[30] Compliance with Court Orders Act of 2016, 114th Cong. § 3(a) (2016) (Discussion Draft), https://web.archive.org/web/20160413195503/https://www.burr.senate.gov/imo/media/doc/BAG16460.pdf [https://perma.cc/7E6T-NRJP].

[31] The bill defined "covered entity" as "a device manufacturer, a software manufacturer, an electronic communication service, a remote computing service, a provider of wire or electronic communication service, a provider of a remote computing service, or any person who provides a product or method to facilitate a communication or the processing or storage of data." Id. § 4(4).

[32] Id. § 3(a)(2).

[33] Id. § 4(12).

[34] Id. § 3(a)(3).

Widespread controversy surrounded the bill even before an official draft was released to the public, and within weeks of the bill's introduction, it was already given "poor odds of passing."[35] The bill's critics primarily asserted it would make Americans' private communications less secure.[36] They also argued that the bill would not be effective in preventing criminals from "going dark" and hiding illegal activities.[37] In response, the bill's sponsors' offices circulated a series of proposed revisions.[38] However, even with the proposed changes, critics argued the legislation would require technologies to be built in such a way that would open the door for bad actors to access user information.[39] One of the bill's fiercest critics came from within the Senate. A press release from the office of U.S. Senator Ron Wyden (D-OR) alleged that the

[35] See Riana Pfefferkorn, The Burr-Feinstein Crypto Bill Would Gut Our Cybersecurity, SLS Blogs: Legal Aggregate (Apr. 26, 2016), https://law.stanford.edu/2016/04/26/the-burr-feinstein-crypto-bill-would-gut-our-cybersecurity/ [https://perma.cc/5EQG-YPCD]; Susan Hennessey, Draft Feinstein-Burr Encryption Bill is Here, Lawfare (Apr. 8, 2016, 11:48 PM), https://www.lawfaremedia.org/article/draft-feinstein-burr-encryption-bill-here [https://perma.cc/8DCT-LLJ5]; Cindy Cohn, The Burr-Feinstein Proposal is Simply Anti-Security, Elec. Frontier Found. (Apr. 8, 2016), https://www.eff.org/deeplinks/2016/04/burr-feinstein-proposal-simply-anti-security [https://perma.cc/FT3F-794U]; BSA | The Software Alliance Statement on Burr-Feinstein Draft Encryption Bill, BSA | Software All. (Apr. 12, 2016), https://www.bsa.org/news-events/news/bsa-the-software-alliance-statement-on-burr-feinstein-draft-encryption-bill [https://perma.cc/C4VF-B68X]; Dustin Volz, Mark Hosenball & Joseph Menn, Push for Encryption Law Falters Despite Apple Case Spotlight, Reuters (May 27, 2016, 8:27 AM), https://www.reuters.com/article/usa-encryption-legislation-idUSL2N18O0BM/ [https://perma.cc/DNG3-QNF5] ("Now, only months later, much of the support is gone, and the push for legislation dead, according to sources in congressional offices, the administration and the tech sector.").

[36] See Riana Pfefferkorn, Here's What the Burr-Feinstein Anti-Crypto Bill Gets Wrong, Just Sec. (Apr. 15, 2016), https://www.justsecurity.org/30606/burr-feinstein-crypto-bill-terrible/ [https://perma.cc/GSK2-CZV7]; David Auerbach, There is No Good Argument for Encryption Backdoors, Slate (Nov. 19, 2015, 4:53 PM), http://www.slate.com/articles/technology/bitwise/2015/11/encryption_backdoors_won_t_make_us_safer_from_terrorism_john_brennan_john.html [https://perma.cc/ZLJ2-JDUH]; Anti-Encryption Bill is an Affront to Privacy, Technological Security, FreedomWorks (Apr. 13, 2016), http://www.freedomworks.org/content/anti-encryption-bill-affront-privacy-technological-security [https://perma.cc/ZK39-KRLS].

[37] See Shane Tews, The FBI Overstated the 'Going Dark' Problem, and the Facts on Encryption Remain the Same, Am. Enter. Inst. (May 24, 2018), https://www.aei.org/technology-and-innovation/the-fbi-overstated-the-going-dark-problem-and-the-facts-on-encryption-remain-the-same/ [https://perma.cc/VYE2-4NA9].

[38] Julian Sanchez, Feinstein-Burr 2.0: The Crypto Backdoor Bill Lives On, Just Sec. (Sept. 9, 2016), https://www.justsecurity.org/32818/feinstein-burr-2-0-crypto-backdoor-bill-lives/ [https://perma.cc/G8UX-9A7U].

[39] Id.

legislation "would effectively outlaw Americans from protecting themselves," and the bill "would leave Americans more vulnerable to stalkers, identity thieves, foreign hackers and criminals."[40]

During the same Congress, then-U.S. House Homeland Security Committee Chairman Michael McCaul (R-TX) and Senator Mark Warner (D-VA) introduced bipartisan, bicameral legislation that would have created a commission modeled after the National Commission on Terrorist Attacks Upon the United States ("9/11 Commission").[41] The proposed commission would be composed of various relevant stakeholders, including technology industry executives, privacy advocates, cryptologists, law enforcement officials, and members of the intelligence community.[42] The reach of the McCaul-Warner bill was broader than the Burr-Feinstein legislation, extending well beyond encryption and focusing on security maintenance more generally.[43] However, it too faced criticism from privacy advocates, who expressed concerns that law enforcement would have unequal representation on the commission and that the bill would provide Congress with an excuse to postpone future action on the issue.[44] Like the Burr-Feinstein bill, the Warner-McCaul bill failed to pass.[45]

[40] Wyden Statement on Burr-Feinstein Anti-Encryption Bill, U.S. Sen. Ron Wyden of Or. (Apr. 13, 2016), https://www.wyden.senate.gov/news/press-releases/wyden-statement-on-burr-feinstein-anti-encryption-bill#:~:text=This%20legislation%20would%20effectively%20outlaw,thieves%2C%20foreign%20hackers%20and%20criminals.. [https://perma.cc/MZT7-XAWV].

[41] Warner, McCaul Lead Bipartisan Coalition to Establish National Commission on Digital Security, Mark R. Warner (Feb. 29, 2016), https://www.warner.senate.gov/public/index.cfm/2016/2/warner-mccaul-lead-bipartisan-coalition-to-establish-national-commission-on-digital-security [https://perma.cc/ 5CV2-M34T]; Erin Kelly, Bipartisan Encryption Bill Seeks to End Feud Between FBI, Tech Industry, USA Today (Feb. 26, 2016, 2:02 PM), https://www.usatoday.com/story/news/2016/02/24/bipartisan-encryption-bill-seeks-end-feud-between-fbi-tech-industry/80849930/ [https://perma.cc/VSC7-9CTG].

[42] Warner, McCaul Lead Bipartisan Coalition to Establish National Commission on Digital Security, supra note 41.

[43] See id.

[44] Dustin Volz & Mark Hosenball, Senate Proposal on Encryption Gives Judges Broad Powers, Reuters (Mar. 21, 2016, 6:21 PM), https://www.reuters.com/article/us-apple-encryption-legislation-idUSKCN0WN2B1/ [https://perma.cc/ESF6-NDE9].

[45] H.R. 4651—Digital Security Commission Act of 2016, Congress.gov, https://www.congress.gov/bill/114th-congress/house-bill/4651/all-actions [https://perma.cc/W9N9-GCPW] (last visited Feb. 19, 2024); S.2604—Digital Security Commission Act of 2016, Congress.gov, https://www.congress.gov/bill/114th-congress/senate-bill/2604 [https://perma.cc/LWJ6-RUBV] (last visited Feb. 19, 2024).

C. The Private Sector's Lingering Need for Congressional Direction in the Face of Increased E2EE Implementation

Today, the encryption debate lingers, but congressional attention to the issue has waned. According to one scholar, public debate concerning encrypted devices "ended . . . not with a bang, but with a whimper."[46] Scholarly articles weighing in on the debate have largely fallen off.[47] Legislative inaction has resulted in long-standing uncertainty for technology companies, courts, and the American public. But no matter one's position on the best path forward, there is no denying that the lack of any resolution to the debate is substantial, and the lingering questions that result are consequential. In 2022 alone, federal and state judges authorized 2,406 wiretaps, 478 of which included instances of encrypted communications.[48] Approximately 92 percent of those communications could not be decrypted by law enforcement.[49]

The impact of E2EE on daily life will only continue to grow. At the end of 2022, Apple announced it was launching expanded E2EE protections for its iCloud service. A year later, Meta announced plans to expand E2EE on Messenger, making its security features more in line with Meta's WhatsApp.[50] According to Loredana Crisan, the head of Messenger, "nobody, including Meta, can see what's sent or said, unless you choose to report the message to us."[51] Google has also adopted E2EE

[46] Riana Pfefferkorn, The Encryption Debate: All Quiet on the Western Front?, Just Sec. (July 6, 2016), https://www.justsecurity.org/31860/encryption-debate-quiet-western-front/ [https://perma.cc/N4WS-E3Z4].

[47] But see Jacob Zarefsky, The Precarious Balance Between National Security and Individual Privacy: Data Encryption in the Twenty-First Century, 23 Tul. J. Tech. & Intell. Prop. 179, 179–80 (2021); Anthony G. Volini, A Deep Dive into Technical Encryption Concepts to Better Understand Cybersecurity & Data Privacy Legal & Policy Issues, 28 J. Intell. Prop. L. 291, 298 (2021); Rafita Ahlam, Note, Apple, the Government, and You: Security and Privacy Implications of the Global Encryption Debate, 44 Fordham Int'l L.J. 771, 775–77 (2021).

[48] Kristin Finklea, Cong. Rsch. Serv., IF11769, Law Enforcement and Technology: The "Lawful Access" Debate (2024).

[49] Id.

[50] Loredana Crisan, Launching Default End-to-End Encryption on Messenger, Meta (Dec. 6, 2023), https://about.fb.com/news/2023/12/default-end-to-end-encryption-on-messenger/ [https://perma.cc/DG8X-PXZQ]; Jonathan Vanian, Meta to Expand Encryption on Messenger Making it Similar to WhatsApp, CNBC (Dec. 7, 2023, 4:52 AM), https://www.cnbc.com/2023/12/07/meta-to-expand-encryption-on-messenger-making-it-similar-to-whatsapp.html [https://perma.cc/Y5LM-MWGJ].

[51] Crisan, supra note 50.

for its Messages application.[52] Furthermore, a project manager at Google has announced plans to add E2EE to Google Authenticator "down the line."[53] These applications also join Signal, a platform on which even the app makers are barred from accessing the encrypted content.[54]

Especially given the rapid advancement of encryption technologies and widespread use of E2EE systems, Congress should renew its focus on considering proposals to either expand or limit law enforcement's access to information. Congress also should clearly define the requirements placed upon technology companies in providing specified information to law enforcement. Without guidance on the extent to which companies must share information with law enforcement, uncertainty will only increase in the face of rapidly advancing technologies, compromising both security and privacy in the process.

II. HOW OTHER FIVE EYES COUNTRIES' RESPONSES TO THE DEBATE SHED LIGHT ON A PATH FORWARD

Fortunately, Congress is not left in the dark in addressing the "going dark" debate. The U.S. has an opportunity to learn from statutes passed in other Five Eyes[55] countries and should consider their respective successes and weaknesses.

A. Australia's Approach: The Telecommunications and Other Legislation Act

In 2018, the Australian Parliament passed the Telecommunications and Other Legislation (Assistance and Access) Act ("TOLA")[56]—the most pro-law enforcement cryptography statute enacted by the Five Eyes thus

[52] Use End-to-End Encryption in Google Messages, Google Messages, https://support.google.com/messages/answer/10252671?hl=en [https://perma.cc/7Z9J-4BYG] (last visited Jan. 31, 2024).

[53] Christiaan Brand (@christiaanbrand), X (Apr. 26, 2023, 1:38 PM), https://twitter.com/christiaanbrand/status/1651279689040920576?s=20 [https://perma.cc/52GQ-Q5TF].

[54] How Do I Know My Communication is Private?, Signal Support, https://support.signal.org/hc/en-us/articles/360007318911-How-do-I-know-my-communication-is-private [https://perma.cc/KTM9-EH88] (last visited Jan. 31, 2024).

[55] The Five Eyes is an intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom, and the United States. Five Country Ministerial, Gov't of Can. (Dec. 15, 2023), https://www.publicsafety.gc.ca/cnt/ntnl-scrt/fv-cntry-mnstrl-en.aspx [https://perma.cc/4GMZ-ZSJ4].

[56] Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth) (Austl.) [hereinafter TOLA].

far. When introducing the bill, Peter Dutton, the Minister for Home Affairs, described E2EE as "eroding the capacity of Australia's law enforcement and security agencies to investigate serious criminal conduct and protect Australians."[57] The legislation passed quickly, despite the controversy surrounding it.[58]

Schedule 1 of TOLA provides Australian law enforcement with three ways of seeking assistance from communications companies.[59] The first option is voluntary, giving the company flexibility to choose whether to comply.[60] The second way—Technical Assistance Notices ("TANs")—are compulsory orders issued by the head of an interception agency or other intelligence agency.[61] They require the communications provider to turn over decrypted information to law enforcement if the company's current technological capabilities allow them to do so.[62] Similarly, the third way—Technical Capability Notices ("TCNs")—are compulsory orders issued jointly by the Attorney-General and the Minister for Communications at the request of the head of a law enforcement agency or other intelligence agency.[63] Unlike TANs, however, TCNs require a communications provider to build the capability to provide assistance to law enforcement if current technology does not permit the provider to grant access.[64]

The authority granted under a TCN is not unlimited, however. The government cannot require a service provider to implement a "backdoor" that would introduce a "systemic weakness" that "affects a whole class of

[57] Keiran Hardy, Australia's Encryption Laws: Practical Need or Political Strategy? 9 Internet Pol'y Rev. 1, 5 (2020).

[58] See George Robert Barker, William Lehr, Mark Loney & Douglas Sicker, The Economic Impact of Laws that Weaken Encryption 4 (2021), https://www.internetsociety.org/wp-content/uploads/2021/05/The_Economic_Impact_of_Laws_that_Weaken_Encryption-EN.pdf [https://perma.cc/42KN-GWGF]; Stilgherrian, Carnegie Endowment for Int'l Peace, The Encryption Debate in Australia: 2021 Update 1 (Mar. 2021), https://carnegieendowment.org/files/202104-Australia_Country_Brief.pdf [https://perma.cc/SA8J-GTJ4]; Hardy, supra note 57, at 5.

[59] Assistance and Access: A New Industry Assistance Framework, Austl. Gov't: Dep't of Home Affs., https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/assistance-and-access-industry-assistance-framework [https://perma.cc/QT36-H6FP] (last visited Jan. 31, 2023); TOLA (Cth) sch 1 (Austl.).

[60] Assistance and Access: A New Industry Assistance Framework, supra note 59.

[61] Id.

[62] Id.

[63] Id.

[64] Id.

technology."[65] In other words, a TCN cannot be used to require a provider to build a capability to decrypt information or remove electronic protection from a whole class of phones, or some other technology group. Instead, the law restricts use of TCNs to situations where a provider is compelled to employ a "targeted weakness" upon a particular individual's device, such as one person's phone.[66]

In 2019, the Parliamentary Joint Committee on Intelligence and Security asked the Australian Independent National Security Legislation Monitor to investigate whether TOLA contained appropriate safeguards for protecting the rights of individuals and whether those concerns were adequately balanced against the countervailing national security concerns.[67] In its review of TOLA's Schedule 1 provisions, the Monitor seemingly validated three widely expressed criticisms of the legislation.[68] First, the Monitor noted that Schedule 1 does not require independent judicial authorization for the coercive TANs and TCNs.[69] As the report noted, "[n]either TCNs nor TANs follow the more usual route . . . of having an independent judicial officer" issuing the instrument.[70] Instead, after the head of a law enforcement agency determines the assistance of a communications provider is "reasonable and proportionate" and compliance would be "practicable" and "technically feasible," no subsequent independent judicial approval is required.[71]

The Monitor's report also concluded that Schedule 1 of TOLA failed to sufficiently define key technical terms like "serious offen[s]e" and "systemic weakness."[72] Under the Act, TANs and TCNs can be issued for domestic criminal law purposes if they relate to a "serious offen[s]e," meaning an offense punishable by three or more years' imprisonment.[73] The Monitor's report confirmed the critique that this definition was overly

[65] Id.

[66] Id.

[67] James Renwick, Indep. Nat'l Sec. Legis. Monitor, Trust but Verify: A Report Concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and Related Matters 5 (2020), https://www.inslm.gov.au/sites/default/files/2020-07/INSLM_Review_TOLA_related_matters.pdf [https://perma.cc/R25Q-H43B].

[68] Id. at 28.

[69] Id. at 191.

[70] Peter Alexander Earls Davis, Decrypting Australia's 'Anti-Encryption' Legislation: The Meaning and Effect of 'Systemic Weakness' Limitation, 44 Comput. L. & Sec. Rev. 1, 8 (2022).

[71] Stilgherrian, supra note 58, at 2.

[72] Renwick, supra note 67, at 24–25, 236.

[73] Id. at 234.

broad, saying that the definition of "serious offen[s]e" should be limited to crimes subject to punishments higher than just three years given the potential security consequences of infiltrating public technology.[74] The report further noted that the statute lacks any substantive definition or examples indicating what would qualify as introducing a "systemic weakness."[75] Accordingly, "[t]he apparent intention of the provision [was] to permit one-off requests or demands for 'exceptional access' to plaintext whilst precluding the mandatory insertion of so-called 'encryption backdoors' or 'security backdoors' by providers into their products on a wholesale basis."[76] However, the legislation does not list any examples of what would create a "systemic weakness," so it is not clear the legislation accomplishes this goal.

The report also highlighted that Schedule 1 does not set up a system for independent technical assessment of proposed notices.[77] Because the heads of law enforcement agencies issue the TANs and TCNs, there are no unbiased technical experts reviewing the issuance of notices.[78] To correct this problem, some have argued that law enforcement should be required to obtain approval from an independent agency of technical expertise before issuing industry assistance notices.[79]

While the independent report outlined weaknesses of the law, the Monitor also determined that such a law was likely needed. The report concluded that "TOLA is or is likely to be necessary" because "the 'right to privacy' is never absolute" and "just as we do not accept lawlessness in the physical world, we should not accept lawlessness in the virtual world."[80]

B. The U.K.'s Approach: The Online Safety Act

In October 2023, the U.K. followed Australia's lead and became the second Five Eyes country to pass legislation governing law enforcement access to encrypted content.[81] The U.K. Parliament passed legislation

[74] Id. at 234–37.
[75] Id. at 209.
[76] Davis, supra note 70, at 5.
[77] Id. at 211.
[78] Id. at 212.
[79] Id.
[80] Id. at 24, 34, 138.
[81] Peter Guest, The UK's Controversial Online Safety Act is Now Law, Wired (Oct. 26, 2023, 8:44 AM), https://www.wired.com/story/the-uks-controversial-online-safety-act-is-now-law/ [https://perma.cc/C6MV-LY3S].

specifically aimed at protecting its citizens from illegal content online, with a focus on protecting children from potentially harmful online content and activity.[82] The law requires social media platforms to remove illegal content and imposes large financial penalties of up to £18 million if they fail to do so.[83]

Early in the legislative process, the bill's fiercest critics dubbed Section 122 of the Act the "spy clause" because it would have required technology companies to create and use software that decrypts communications in order to identify prohibited content.[84] Specifically, Section 122 of the Act would have empowered the U.K. government's communications regulator, Ofcom, to require regulated platforms to identify certain content and prevent people from accessing it.[85] But, in the face of mounting criticism, the U.K. government announced it would not use these controversial powers prescribed in the provision, at least temporarily.[86] Junior Arts and Heritage Minister Lord Stephen Parkinson announced that Ofcom would only require companies to scan their networks for harmful content when "technically feasible."[87] He said, "A notice can only be issued . . . where technology has been accredited as meeting minimum standards of accuracy in detecting only child sexual abuse and exploitation content."[88] This notice placated the concerns of several technology companies, including Meta's WhatsApp and Signal,

[82] Id.

[83] UK Online Safety Act Becomes Law, Hunton Andrews Kurth (Oct. 27, 2023), https://www.huntonprivacyblog.com/2023/10/27/uk-online-safety-act-becomes-law/ [https://perma.cc/XX5X-WWZM].

[84] See UK: 'Spy Clause' in Online Safety Bill Must be Addressed Before it Becomes Law, Amnesty Int'l (Sept. 5, 2023), https://www.amnesty.org/en/latest/news/2023/09/uk-spy-clause-in-online-safety-bill-must-be-addressed-before-it-becomes-law/ [https://perma.cc/4VWN-TQRG].

[85] Stewart Room, Will U.K. Online Safety Bill Break Encryption for Mass Surveillance?, Forbes (Sept. 21, 2023, 5:09 AM), https://www.forbes.com/sites/stewartroom/2023/09/21/will-uk-online-safety-bill-break-encryption-for-mass-surveillance/?sh=651339ca40f0 [https://perma.cc/ZMM6-3K72].

[86] Natasha Lomas, Ministerial Statement on UK's Online Safety Bill Seen as Steering Out of Encryption Clash, TechCrunch (Sept. 7, 2023, 3:12 PM), https://techcrunch.com/2023/09/06/osb-encryption-scanning-feasibility/ [https://perma.cc/GE4C-BQM6].

[87] Tom Jowitt, Government Abandons Plan to Scan Encrypted Messages, Silicon (Sept. 7, 2023, 9:27 AM), https://www.silicon.co.uk/e-management/social-laws/government-abandons-plan-to-scan-encrypted-messages-528371#:~:text=The%20FT%20reported%20that%20in,was%20capable%20of%20doing%20so [https://perma.cc/49F4-7UMD].

[88] Cristina Criddle, Anna Gross & John Aglionby, UK Pulls Back from Clash with Big Tech Over Private Messaging, Fin. Times (Sept. 6, 2023), https://www.ft.com/content/770e58b1-a299-4b7b-a129-bded8649a43b [https://perma.cc/A89L-T3J4].

who had promised to leave the U.K. if forced to align with Section 122.[89] Until enforcement of Section 122 becomes "technically feasible," its practical consequences on technology companies in the U.K. appear minimal.

III. A FLEXIBLE LEGISLATIVE APPROACH TO THE ENCRYPTION DEBATE

The Five Eyes' struggles and Congress's inability to pass viable legislation to address the encryption debate proves there are no easy solutions. Future actions to address the encryption debate should look to both the Australian and the U.K. laws for guidance, but legislators should heed the warnings from the critics of those approaches. Lessons from these countries' efforts, as well as Congress's past gridlock on the issue, counsel in favor of pursuing a more flexible approach.

Future legislation could aid in balancing the tradeoff between protecting user security and ensuring public safety by incentivizing innovation among private companies. In a perfect world, these competing concerns would not be in conflict, meaning technology could hypothetically provide a way for law enforcement to have exceptional access without compromising user security. Considering some experts believe developing such technology is indeed feasible, this world might one day become a reality. However, even assuming such technology is possible to develop, current incentives dissuade companies from pursuing such innovation. In general, large communications providers advertise E2EE as a major benefit for the consumer. They know their consumers want their privacy protected to the fullest extent possible. Therefore, using E2EE that prevents even the companies themselves, much less law enforcement, from accessing users' communications likely appeals to their consumer base. Ultimately, developing the technology to allow for exceptional access runs counter to technology companies' marketing and profitability goals, which are achieved by prioritizing user security. Companies' inability to access data is a feature that the companies tout and on which consumers rely.

Neither Australia's law nor the U.K.'s law attempted to adjust this existing incentive structure. While Australia's law purports to provide the

[89] See WhatsApp and Other Messaging Apps Oppose UK's Move on Encryption, Reuters (Apr. 18, 2023, 4:57 PM), https://www.reuters.com/technology/whatsapp-other-messaging-apps-oppose-uks-move-encryption-2023-04-18/ [https://perma.cc/W2BS-4ZGZ].

government with the power to force technology companies to grant exceptional access, it does not incentivize companies to develop innovative technologies for gaining such access without creating a systemic weakness. Furthermore, the U.K. law ignores the feasibility of implementation altogether. It runs into the same problem: How can you compel companies to provide law enforcement with exceptional access if they do not have the technological capability to do so? The U.K. Parliament failed to address this question. Now the U.K. is left with a law that cannot be enforced until technology is developed.

There are several ways in which this incentive problem can be solved in the United States, each with its own costs. For one, Congress could fund a research project itself to develop feasible exceptional access technology. However, a congressionally funded research project would be expensive. It may also be politically challenging to garner legislative support for using taxpayer funds for the project. Alternatively, Congress could pass a law requiring technology companies to provide exceptional access into their software or face substantial fines. But provisions imposing fines for noncompliance faced strong criticism in both Australia and the U.K. because the provisions forced these respective governments to weigh in on what constituted noncompliance, requiring technical considerations. For example, what forms of exceptional access would circumvent fine imposition? How much time would the companies have to develop technology allowing access? Would the costs of reengineering a company's system and potentially risking customer dissatisfaction outweigh the costs of a government-imposed fine? What would be considered overly burdensome exceptional access?

In light of these considerations, Congress should consider creating an independent commission tasked with making recommendations to Congress regarding the best approach for crafting legislation to address the debate.[90] Such a commission could be similar to the commission proposed by Congressman McCaul and Senator Warner. It could be composed of a diverse group of stakeholders, including technology experts from both the government and the private sector, law enforcement officials, officials from the intelligence community, cryptologists, and privacy advocates. With such a broad array of stakeholders on the commission weighing in on relevant issues, the commission's discussions

[90] See supra Section I.B (discussing the McCaul-Warner bill which advocated for creating an independent commission modeled after the 9/11 Commission).

could supersede the increasingly polarized and inflammatory rhetoric characterizing the encryption debate. The commission could therefore more effectively reach a nuanced, balanced approach respectful of both law enforcement needs and user security.

The independent commission could be tasked with determining the feasibility of the current exceptional access options. In so doing, the U.S. could avoid making the same mistake as the U.K., where the law was considered unenforceable because its demands were not technically feasible. Congress must recognize its inability to fully understand the complexities of encryption technology, and the independent commission could instead use its members' technical expertise and knowledge of industry demands to make recommendations for a clear, enforceable statute.

Considering the weaknesses of Australia's and the U.K.'s laws, the independent commission should specifically focus on providing Congress with clear and workable definitions for arguably vague technical terms. Such a focus would tackle the problems associated with TOLA's failure to appropriately define terms including "systemic weakness" and "serious offen[s]e." The independent commission could seek to answer questions, such as what types of exceptional access strategies or "backdoors" would count as a "systemic weakness." With its technical expertise, the commission could provide Congress with the information necessary to draft more precise, and therefore more agreeable, language.

In addition to tasking a commission with providing recommendations to Congress on how to best address the issue in the short term, a future proposal should take into account the constantly evolving landscape of encryption technologies. The contours of encryption technology capabilities and risks will not look the same five years from now, or even one year from now. Long-term, independent technical assessment of the laws governing E2EE is essential to ensuring the law keeps pace with rapidly changing technologies.

Therefore, Congress should consider either tasking the commission with providing annual updates and recommendations to Congress or creating an independent agency tasked with confronting these challenges. If an independent agency is created, such an agency would have the flexibility necessary to issue and rescind regulations reflecting future technological advancements that are impossible to currently predict. Such an agency could issue regulations consistent with statutory constraints

imposed by Congress to achieve an appropriate balance between government security needs and individual liberties concerns.

CONCLUSION

The encryption debate may be mostly hidden from the public eye, but the potential legal ramifications of advancing encryption technologies are more salient than ever. This Essay suggests that Congress should consider actions taken by other countries as guidance for how to best proceed. It asserts that a nuanced approach involving a commission of experts from relevant stakeholder groups is the first step. That is not to suggest that such a commission will solve all the delicate considerations arising within the encryption debate. More research on encryption capabilities and the viability of secure exceptional access is necessary. Much more can be written about how to best legislate within this realm, but it is imperative that future proposals take into account the rapidly changing and global nature of the debate.