NOTE

APPLE, THE GOVERNMENT, AND YOU: SECURITY AND PRIVACY IMPLICATIONS OF THE GLOBAL ENCRYPTION DEBATE

Rafita Ahlam[*]

ABSTRACT

In 2013, ex-NSA contractor Edward Snowden leaked information that revealed the extent to which several countries, including the United States, developed a global surveillance system capable of collecting and sharing a massive amount of information. A direct consequence of the Snowden disclosures was the public backlash against large technology companies, who in turn strengthened security measures on consumer smartphones to reduce unauthorized government access. Apple, in particular, designated itself as the company that prioritizes user security and privacy above all, and now boasts some of the strongest encryption measures on the consumer market. This Note addresses the new problem that arose from this development: the clash between law enforcement, which desires probative evidence from encrypted smartphones and entities (including technology companies and users), who have a vested interest in the protection of the data. Described as the "Going Dark" problem or the "Encryption Debate," this Note explores this tension in various jurisdictions and offers important considerations in how a country might ultimately resolve it.

ABSTRACT 771

* J.D. Candidate, 2021, Fordham University School of Law; B.A., 2016, SUNY Binghamton; Writing and Research Editor, *Fordham International Law Journal*, Volume XLIV. First, an immense thank you to Professor Olivier Sylvain for his mentorship and guidance in developing this topic and writing this Note. Thank you to the board and staff members of the Journal who assisted in editing this Note, with a special thank you to my editorial board, Michael Campbell, Noah Parson, Kelsey Halloran, Casey Morin, and last but not least, my partner-in-crime, Marcus Thomas, for their valuable constructive feedback. Last, thank you to my family, friends, and partner for their love and support.

I. INTRODUCTION 773
II. THE FACTS ABOUT ENCRYPTION 777
A. Encryption: Ideologies, Description, and its Use in the iPhone 778
1. The Value of Encryption 778
2. Defining Encryption 781
3. Apple and its Use of Encryption 782
B. The Legitimate Interests of Law Enforcement ... 785
1. National Security 786
2. Local Crimes 790
3. Sexual Exploitation of Minors 791
C. Extraordinary Access and Lawful Hacking 793
III. DISCUSSION OF THE LEGAL INTERNATIONAL LANDSCAPE 797
A. United Kingdom 798
1. The Investigatory Powers Act 798
2. The Data Protection Act & Privacy Expectations for Mobile Data 801
3. Application of the UK Legal Regime to Encrypted Smartphones 802
B. Australia 803
1. The Assistance and Access Bill 804
2. Australian Expectations of Privacy 805
C. Germany 808
1. Lawful Hacking in Germany 809
2. The Fundamental Right to Privacy 810
D. China 813
1. China's Development of Encryption Technologies 814
2. China as a Surveillance State 817
IV. UNITED STATES 820
A. Using the All Writs Act to Compel Apple to Create a Backdoor for the US Government 821
1. Current Jurisprudence on Applying the AWA to iPhones 823
2. The All Writs Act Cannot be Interpreted to Compel Apple to Write Code that Creates a Backdoor for the Government. 826

B. The Fourth Amendment Privacy Implications of Lawful Hacking 829
1. Fourth Amendment Jurisprudence 829
2. Reasonable Expectations of Privacy after *Carpenter* 833
V. LAWFUL HACKING AS THE APPROPRIATE SOLUTION TO THE ENCRYPTION DEBATE..... 835
A. Current US Legislation 836
B. The Normative Argument Against Backdoors.... 838
C. The Normative Argument for Lawful Hacking .. 843
VI. CONCLUSION..... 844

I. INTRODUCTION

In the critically acclaimed television sitcom, *Parks and Recreation*, one of the main characters, Ron Swanson, protects his privacy with a zealous vigor and repudiates the local government's attempts to gather information about his life.[1] Throughout the show, Swanson takes exaggerated efforts to prevent his coworkers from learning anything about him beyond his name, leading to comical interactions with other characters who hold differing opinions on the amount of personal information they are willing to reveal to the world. His battle for his right to privacy falters, however, when a new technology company in town collects and uses the data without any authorization from the user. Though this company is entirely fictional, Swanson's concerns about the unauthorized collection and misuse of his personal information reflect concerns of real individuals. He worries that the collected data might fall into the wrong hands, and for him, the wrong hands often belong to nonsensical bureaucrats.

Parks and Recreation's arc picks up on a trope popularized by George Orwell's *1984*,[2] which depicts a world where technological

1. *See* Adrienne Tyler, *Parks & Recreation: How Old Ron Swanson Is at The Beginning & End*, SCREENRANT (Aug. 1, 2020), https://screenrant.com/parks-recreation-ron-swanson-nick-offerman-age-old/ [https://perma.cc/JXS6-SDDJ]; *see also* Jason Diamond, *Masculinity in the Age of Ron Swanson: The Legacy of* Parks and Recreation*'s Most Iconic Character*, VULTURE (Feb. 3, 2015), https://www.vulture.com/2015/02/parks-and-recreation-ron-swanson-masculinity.html [https://perma.cc/YTY2-2PNP].

2. GEORGE ORWELL, 1984 (1949) (alternatively published as *Nineteen Eighty-Four*). *See, e.g.*, Ian Crouch, *So Are We Living in 1984?*, NEW YORKER MAG. (June 11, 2013),

advances resulted in increased government surveillance and pervasive violations of privacy rights. Nearly thirty years later than Orwell's timeline, in 2013, Edward Snowden exposed the global surveillance state.[3] His disclosures revealed the extent to which the US government had surveilled its citizens, as well as the activities of other governments in collecting data on both their citizens and persons in other countries.[4] The US government deemed this level of surveillance necessary and found that pending threats from foreign actors outweighed the risks to civil liberties.[5]

One of the most shocking revelations was that these governments manipulated existing technology created by prominent companies to gather the information.[6] For companies like Apple, the Snowden disclosures posed a serious problem.[7] To the outside world, technology companies appeared to be eagerly complying with government data-collection programs, and smartphones (like the iPhone), which were intended to help individuals connect, were instead being used as surveillance tools

---

https://www.newyorker.com/books/page-turner/so-are-we-living-in-1984 [https://perma.cc/299D-RJC8]. The novel injected phrases such as "Big Brother is watching you" into popular culture. For an example of its influence on the American judiciary, see Judge Reinhart's dissent in United States v. Kincade, 379 F.3d 813, 842 (9th Cir. 2004). Judge Reinhardt illustrates the concerns of a police state and underlines the importance of adapting the law to today's technology. *Id.*

3. *See* Rachel Taylor, *Intelligence-Sharing Agreements & International Data Protection: Avoiding A Global Surveillance State*, 17 WASH U. GLOB. STUD. L. REV. 731, 731 (2018).

4. *See* Mark Mazetti & Michael Schmidt, *Ex-C.I.A. Worker Says He Disclosed U.S. Surveillance*, N.Y. TIMES, June 10, 2013, at A1, https://www.nytimes.com/2013/06/10/us/former-cia-worker-says-he-leaked-surveillance-data.html?searchResultPosition=7 [https://perma.cc/9DRT-Y7CM]; *Snowden Revelations*, LAWFARE, https://www.lawfareblog.com/snowden-revelations [https://perma.cc/ZV3D-F7LW] (last visited May 31, 2020) (indicating that, for example, the National Security Agency has worked with Australia, Germany, and the United Kingdom).

5. *See* TIMOTHY H. EDGAR, BEYOND SNOWDEN: PRIVACY, MASS SURVEILLANCE, AND THE STRUGGLE TO REFORM THE NSA 17 (The Brookings Inst., 2017).

6. *Snowden Revelations*, *supra* note 4.

7. *See* Kristen Jacobsen, *Game of Phones, Data Isn't Coming: Modern Mobile Operating System Encryption and its Chilling Effect on Law Enforcement*, 85 GEO. WASH. L. REV. 566, 589 (2017) ("Numerous technology companies, including Apple and Google, redesigned their products to include encryption in direct response to Edward Snowden's infamous disclosure regarding the US government's mass surveillance.").

by the government.[8] Subsequent scandals highlighted the abuse of data by malevolent actors when technology companies failed to vigilantly restrict data access.[9] In response to negative public reactions, Apple and other technology companies doubled their commitment to privacy and security by embracing stronger encryption on their products.[10] While the average iPhone user may have been thrilled by the idea that the government could not get into her smartphone so easily,[11] law enforcement officials in varying jurisdictions are now frustrated by the fact that encryption impedes their efforts to solve crimes.[12]

Referred to by some as the "Encryption Debate" and by others as the "Going Dark" problem,[13] this conflict between law

8. Daisuke Wakabayashi, *Apple's Evolution into a Privacy Liner*, WALL ST. J. (Feb. 24, 2016), https://www.wsj.com/articles/apples-evolution-into-a-privacy-hard-liner-1456277659 [https://perma.cc/42L7-7Z8J].

9. *See* Matthew Rosenberg & Gabriel Dance, *Affected Users Say Facebook Betrayed Them*, N.Y. TIMES, Apr. 9, 2018, at A1, https://www.nytimes.com/2018/04/08/us/facebook-users-data-harvested-cambridge-analytica.html [https://perma.cc/E4YF-N75X]. *See also* Emily Stewart, *Mark Zuckerberg said Facebook "made mistakes" on the Cambridge Analytica scandal. He's not apologizing*, VOX (Mar. 21, 2018), https://www.vox.com/technology/2018/3/21/17148852/mark-zuckerberg-facebook-cambridge-analytica-breach. A related issue is the misuse of data by the technology companies themselves, but that issue will not be discussed as it is beyond the scope of the arguments posited here.

10. *See* Wakabayashi, *supra* note 8. *See also* Scott J. Shackelford et al., *iGovernance: The Future of Multi-Stakeholder Internet Governance in the Wake of the Apple Encryption Saga*, 42 N.C. INT'L L. 883, 924 (2017) ("[T]he U.S. government does not seem to fully comprehend how the rules of the game for companies like Apple, Google, Microsoft, and Facebook were changed by those disclosures. In fact, Apple's strong commitment to encryption was likely informed by those revelations."); David Sanger & Brian Chen, *Signaling Post-Snowden Era, New iPhone Locks Out NSA*, N.Y. TIMES, Sept. 27, 2014, at A1, https://www.nytimes.com/2014/09/27/technology/iphone-locks-out-the-nsa-signaling-a-post-snowden-era-.html?_r=1 [https://perma.cc/BYH8-6WNW].

11. *But see* Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 172 (2018) ("Despite all the publicity around security-enhancing technologies, we don't know whether consumers actually care about them – that is, whether they buy the new iPhone because it has end-to-end encryption rather than because it has a bigger screen.").

12. *See* CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE, MOVING THE ENCRYPTION POLICY CONVERSATION FORWARD, 3 (2019) [hereinafter CARNEGIE].

13. *See* Maj. Gen. Charles, J. Dunlap, Jr., Essay, *Social Justice and Silicon Valley: A Perspective on the Apple-FBI Case and the "Going Dark" Debate*, 49 CONN. L. REV. 1685, 1688 (2017); CARNEGIE, *supra* note 12; WASH. POST EDITORIAL BD., Opinion, *Putting the digital keys to unlock data out of reach of authorities*, WASH. POST (July 18, 2015), https://www.washingtonpost.com/opinions/putting-the-digital-keys-to-unlock-data-out-of-reach-of-authorities/2015/07/18/d6aa7970-2beb-11e5-a250-42bd812efc09_story.html [https://perma.cc/V5XH-M3GE].

enforcement and technology companies is currently playing out throughout the world and at the federal, state, and local levels in the United States.[14] In many ways, striking the right balance in providing information to law enforcement while protecting security and privacy interests is an engineering problem, not a legal one.[15] Yet, the "technological arms race"[16] between governments and companies propelled to the front of the debate two significant legal questions on resolving this tension: first, whether the government can compel technology companies like Apple to code backdoors[17] into their smartphones to provide "extraordinary access" to data, and second, whether the use of alternative methods by the government implicates existing privacy rights.

This Note explores and analyzes these questions with a focus on the US approach to extraction of data from encrypted smartphones. This discussion proceeds in five Parts. Part II provides the factual background for the debate: a primer on encryption, interests of law enforcement, and the two technological methods at issue in the debate. Part III explores the current international legal landscape with a focus on the countries that are most vocal in the Encryption Debate: the United Kingdom, Australia, Germany, and China. Part IV discusses US laws and cases on the debate, analyzes the two issues posed above, and provides important considerations and implications for resolving the debate in the United States. Part V argues that the United States should not compel technology companies to provide extraordinary access to smartphones by modifying the encryption code, and should instead utilize other means of procuring data that does not threaten existing security and privacy rights. Part VI concludes by reiterating that lawful hacking is the appropriate solution for the Encryption Debate

14. *See infra* Part III.

15. *See* Steven Levy, *Cracking the Crypto War*, WIRED MAG. (May 25, 2018), https://www.wired.com/story/crypto-war-clear-encryption/ [https://perma.cc/FM9K-N49K]; Steven Bellovin et al., *Analysis of the CLEAR Protocol per the National Academies' Framework*, 3 DEP'T COMPUT. SCI. COLUM. U. 18, 2 (May 10, 2018) (critiquing one proposed engineering option).

16. CYRUS VANCE JR., REPORT OF THE MANHATTAN DISTRICT ATTORNEY'S OFFICE ON: SMARTPHONE ENCRYPTION AND PUBLIC SAFETY 30 (Nov. 2016) [hereinafter VANCE 2016].

17. *See infra* Section II.C.

and that the United States' ultimate choice will have a global impact.

II. THE FACTS ABOUT ENCRYPTION

The term "encryption" evokes images of computer hackers racing against the clock to crack the code and help the suave hero save the world.[18] In reality, encryption refers to a method of data protection wherein said data is scrambled, making it inaccessible to anyone without the "decryption key."[19] The value of encryption depends on the end user, the type of data that needs to be protected, and the complications that may arise when the accessibility of that data becomes strictly limited to specific users. To understand the role of encryption in the debate, this Part provides the factual background giving rise to the tension. Section II.A discusses the ideological underpinnings of encryption and data protection, details on how encryption works, and how Apple[20] uses encryption in its devices. Section II.B

18. For a real-life example of hackers saving the day, consider the hacktivist group, Anonymous. The group espoused libertarian views, sometimes extreme and divisive, but often efforts focused on uncovering and revealing the conduct of malevolent actors. Dale Beran, *The Return of Anonymous,* ATLANTIC (Aug. 11, 2020), https://www.theatlantic.com/technology/archive/2020/08/hacker-group-anonymous-returns/615058/ [https://perma.cc/6HLJ-XQLQ]. Its founder, Aubrey Cottle, has set his sights on dispelling falsehoods spread by QAnon—a group whose supporters have notably manipulated and warped public discourse to the point that the FBI considers it a domestic terror threat. *See* Shawn Langlois, *Founder of hacker group Anonymous reveals his ultimate 'end-game'*, MARKETWATCH (Nov. 2, 2020), https://www.marketwatch.com/story/founder-of-hacker-group-anonymous-reveals-his-ultimate-endgame-11604336926 [https://perma.cc/DDF9-749A]; A.J. Vicens & Ali Breland, *QAnon is Supposed to Be All About Protecting Kids. Its Primary Enabler Appears to Have Hosted Child Porn Domains*, MOTHER JONES (Oct. 29, 2020), https://www.motherjones.com/politics/2020/10/jim-watkins-child-pornography-domains/ [https://perma.cc/TB9U-P2Q4]; Kevin Roose, *What is QAnon, the Viral Pro-Trump Conspiracy Theory?*, N.Y. TIMES (Jan. 17, 2021), https://www.nytimes.com/article/what-is-qanon.html [https://perma.cc/F9H3-TTBN].

19. *See* Paul Ohm, *Good Enough Privacy*, 1 U. CHI. LEGAL FORUM 1, 9 (2008) [hereinafter Ohm, *Good Enough*]; *see also* Whitson Gordon, *The One Thing that Protects a Laptop After It's Been Stolen*, N.Y. TIMES, Mar. 13, 2018, at B6, https://www.nytimes.com/2018/03/13/smarter-living/how-to-encrypt-your-computers-data.html [https://perma.cc/B6TB-KD54].

20. The analysis in the Note applies to all technology companies, but will use Apple as example given its prevalence in the industry. Apple boasts has the strongest encryption software on the consumer market. *See* Matt Burgess, *Apple's privacy strength is also one of its greatest weaknesses*, WIRED MAG. (May 21, 2020), https://www.wired.co.uk/article/apple-

discusses the legitimate interests of law enforcement in preventing and resolving crimes and how encryption serves as a barrier to those interests. Section II.C presents and explains two technological mechanisms used by law enforcement as workarounds to encrypted smartphones, and will lay the foundation for the discussion and analysis of its legal implications in later Parts.

A. Encryption: Ideologies, Description, and its Use in the iPhone

1. The Value of Encryption

The desire to protect personal data—and the corollary need to build the infrastructure that controls information flows—seems intuitive,[21] or at least reasonable in an age when technology companies are constantly challenged on their duties to their users.[22] Encryption, a form of data protection, is primarily used in two ways: privacy and cybersecurity. Though the terms privacy and cybersecurity are often used interchangeably, issues of data privacy are different from those of cybersecurity.[23] Data protection and data privacy refers to ensuring the privacy of personal information through laws regulating the collection, use, and control of personal data,[24] whereas cybersecurity is narrower and refers specifically to the infrastructure built to secure data, personal or non-personal.[25] Both have the goal of securing data,

---

security-privacy-competitive-advantage [https://perma.cc/SS5X-L26W]. Other prominent technology companies, including Google and Huawai, also offer encryption on their devices. *See* Eric Manpearl, *The International Front of the Going Dark Debate*, 22 VA. J.L. & TECH. 158, 162 (2019); Jacobsen, *supra* note 7, at 575.

21. *See generally* Louis Brandeis & Samuel Warren, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

22. Shira Ovide, *Congress Agrees: Big Tech is Broken*, N.Y. TIMES (Oct. 7, 2020), https://www.nytimes.com/2020/10/07/technology/congress-big-tech.html [https://perma.cc/JX9Q-CB9T]; *4 Key Takeaways from Washington's Big Tech Hearing on 'Monopoly Power'*, NPR (July 30, 2020), https://www.npr.org/2020/07/30/896952403/4-key-takeaways-from-washingtons-big-tech-hearing-on-monopoly-power [https://perma.cc/Z67X-DNM4].

23. *See* William McGeveran, *The Duty of Data Security*, 103 MIN. L. REV. 1135, 1141 (2019).

24. *See* Ohm, *Good Enough*, *supra* note 10, at 7-8; McGeveran, *supra* note 23, at 1141.

25. *See* McGeveran, *supra* note 23, at 1141.

and encryption serves as one of several methods to prevent the unauthorized collection of data.[26]

Some entities value encryption because it is a form of cybersecurity.[27] Banks, businesses, and pharmaceutical companies are illustrative of some entities that have an interest in protecting their trade secrets and proprietary information from hackers and other bad actors.[28] At a more granular level, encryption ensures that the everyday computer user may enter credit card information at the payment page of, for example, a hotel website, without the concern that the information is being stolen or misappropriated.[29] Data breaches at large companies, including Target and Equifax, resulted in the release of information such as social security numbers, mailing addresses, and other confidential records.[30] Even the US federal government is susceptible to cyberattacks: in 2015, the Office of Personnel Management suffered a data breach that resulted in the data of over 4.2 million employees being stolen.[31] As demonstrated by these examples, encryption matters in ensuring that such confidential information is kept secure and private by the entities entrusted to hold it.[32] Moreover, encryption is a necessary step in preventing sensitive and confidential information from getting into the hands of malicious actors and hackers.[33]

---

26. *See* Ohm, *Good Enough*, *supra* note 19, at 9-10.

27. *See* John Mylan Traylor, Note, *Shedding Light on the "Going Dark Problem" and the Encryption Debate*, 50 U. MICH. J. L. REFORM 489, 491-92 (2016).

28. *See* Erick S. Lee & Adam R. Pearlman, *National Security, Narcissism, Voyeurism, and* Kyllo*: How Intelligence Programs and Social Norms are Affecting the Fourth Amendment*, 2 TEX. A&M L. REV. 719, 763 (2015).

29. *See, e.g.*, Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236, 257 (3rd Cir. 2015) (finding that a hotel chain's failure to secure consumer credit card information had monetary implications for consumers and credit card companies).

30. Rachel Abrams, *Target to Pay $18.5 Million to 47 States in Security Breach Settlement*, N.Y. TIMES (May 23, 2017), https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html [https://perma.cc/VG9A-86UW]; *Equifax Data Breach Settlement*, FED. TRADE COMM'N, https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement [https://perma.cc/R97E-AGYA] (last visited Jan. 24, 2021).

31. *Cybersecurity Resource Center: Cybersecurity Incidents*, OFF. PERS. MGMT., https://www.opm.gov/cybersecurity/cybersecurity-incidents/ [https://perma.cc/V6E8-RXF4] (last visited Feb. 26, 2021).

32. *See* Lee & Pearlman, *supra* note 28, at 758.

33. *See* Traylor, *supra* note 27, at 493.

Others use encryption because they value their privacy and are interested in controlling the distribution of information about themselves.[34] Facebook users, for example, were furious when they found out their personal information was released to a third-party, who then exploited that information by tailoring deceptive advertisements and false news articles to ultimately influence their votes in the 2016 US presidential elections.[35] To some, privacy allows an individual to explore her capacity for self-determination, autonomy, and worth.[36] It creates a sphere where a person can engage in the process of identifying conceptions of herself or define her intimate relationships to others.[37] Here, encryption is a tool that provides a person the security she desires in controlling who has access to information about herself.

Last, some value encryption as a form of protection from government surveillance and state control of personal data.[38] As the entity with a monopoly on legitimate violence, the government can exact punishment or sanctions that other actors cannot.[39] Encryption, thus, is necessary to secure protection from government abuses. Privacy scholars argue that individuals are free to generate ideas when the government is not involved given that government oversight may instead lead to a chilling effect on speech, free expression, or other limitations on civil rights.[40] Where some see the oversight as necessary to incentivize good behavior and to hold individuals or entities accountable for their actions,[41] others advance the notion that democracy is more

34. Julia Carrie Wong & Matthew Cantor, *How to speak Silicon Valley: 53 essential tech-bro terms explained*, GUARDIAN (June 27, 2019), https://www.theguardian.com/us-news/2019/jun/26/how-to-speak-silicon-valley-decoding-tech-bros-from-microdosing-to-privacy [https://perma.cc/7ABP-3BXZ] ("privacy (n) – *Archaic*. The concept of maintaining control over one's personal information.").

35. *See* CARNEGIE, *supra* note 12.

36. *See* Ohm, *Good Enough*, *supra* note 19, at 21.

37. *See* Griswold v. Connecticut, 381 U.S. 479, 484 (1965) (stating that the US Constitution creates zones, or penumbras, of privacy).

38. *See* Rozenshtein, *supra* note 11, at 121; Olivia Gonzalez, *Cracks in the Armor: Legal Approaches to Encryption*, 2019 U. ILL. J.L. TECH. & POL'Y 1, 9 (2019).

39. André Munro, *State Monopoly on Violence*, ENCYCLOPEDIA BRITANNICA, https://www.britannica.com/topic/state-monopoly-on-violence (last visited Jan. 24, 2021).

40. *See* Ohm, *Good Enough*, *supra* note 19, at 22; Gonzalez, *supra* note 38, at 4 ("unburdened by the chilling effect of surveillance").

41. Tom Huddleston Jr., *Bill Gates: 'Government needs to get involved' to regulate big tech companies*, CNBC (Oct. 17, 2019), https://www.cnbc.com/2019/10/17/bill-gates-

effective when citizens are free to make decisions without government oversight.[42] In this regard, privacy from government intrusion is necessary for dissidents or freedom fighters who seek to reform civil society without the fear of repercussions from their respective governments.[43] In less contentious settings, many, including industry leaders in Silicon Valley, view encryption as necessary to balance against surveillance technology used by law enforcement and restore the playing field to pre-digital-age levels.[44] Encryption returns to some the option to control how their personal information is used as technological advances threaten the surrender of that control.[45]

2. Defining Encryption

Encryption is a catch-all term used to refer to a method of data protection wherein said data is scrambled, making it inaccessible to anyone without a "decryption key" (the code that would unlock the encryption).[46] Unlike typical password protection, encryption is coded in such a way that it is theoretically impossible for the average user to break the encryption without a decryption key. [47] Thus, encryption offers a reasonable amount of confidentiality to its users. However, it is important to distinguish the different types of encryption and

government-needs-to-regulate-big-tech-companies.html [https://perma.cc/NQQ5-76VU].

42. *See* Ohm, *Good Enough, supra* note 19, at 62.

43. *See* Ohm, *Good Enough, supra* note 19, at 20; Rozenshtein, *supra* note 11, at 119.

44. *See* Rozenshtein, *supra* note 11, at 119; THERESA M. PAYTON & THEODORE CLAYPOOLE, PRIVACY IN THE AGE OF BIG DATA 237 (Rowman & Littlefield publ. 2014).

45. *See* Rozenshtein, *supra* note 11, at 177 ("Only a few companies . . . are willing to say what many engineers feel: government surveillance has become excessive, and the playing field needs to be rebalanced in the direction of user privacy.").

46. As Section II.B discusses, decryption is not an impossible feat—rather, it is about the resources and capabilities available to decrypt the device. For example, a major project at the NSA is to circumvent encryption measures. *See* Nicole Perlroth et al., *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*, N.Y. TIMES, Sept. 5, 2013, at A1, https://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html [https://perma.cc/R56Z-KSR7]; *see also* Bruce Schneier, *NSA surveillance: A guide to staying secure,* GUARDIAN (Sept. 6, 2013), https://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance [https://perma.cc/QVT2-CPKE].

47. *See* Ohm, *Good Enough, supra* note 19, at 9. The terms "encryption" and "encrypted" are used interchangeably in the Encryption Debate.

how each type is applied to tangible products and intangible services.

The two main types of encryption are "end-to-end encryption" (or "double encryption") and "device encryption" (or "full-disk encryption").[48] End-to-end encryption refers to data that can only be decrypted by the original sender and the intended recipient.[49] End-to-end encryption is applied to protect "data-in-motion,"[50] or data that is being shared with others, including text messages and emails. Many communication services, like WhatsApp and Facebook Messenger, use end-to-end encryption to ensure that the only people who can access communications are the sender(s) and recipient(s).[51] Device encryption, on the other hand, refers to a type of encryption where the decryption key exists only on the locked device.[52] Device encryption protects "data-at-rest," which is data that is not being shared with others in the way that data-in-motion is.[53] Device encryption can be used to encrypt external hard drives and other devices.[54] This Note focuses on the latter type of encryption and will explain in later sections why in some contexts data derived from an encrypted smartphone is different from data derived from encrypted communications on that smartphone.

3. Apple and its Use of Encryption

Apple is a technology company with global operations founded in the United States and whose devices are available in several major international markets.[55] Its products and services dominate a significant share in the markets of each jurisdiction

48. *See* Jacobsen, *supra* note 7, at 574.

49. *See* Robert J. Anello & Richard F. Albert, *The International Encryption Debate: Privacy Versus Big Brother*, 261 N.Y. L.J. (June 12, 2019).

50. *See* Manpearl, *supra* note 20, at 160; Rozenshtein, *supra* note 11, at 135.

51. *See* Andy Greenberg, *Hacker Lexicon: What is End-to-End Encryption?*, WIRED MAG. (Nov. 25, 2014), https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/ [https://perma.cc/FD3Z-8574].

52. *See* Manpearl, *supra* note 20, at 160.

53. *See* Anello & Albert, *supra* note 49.

54. *Id.*

55. *Apple, Inc.*, CNN, https://money.cnn.com/quote/profile/profile.html?symb=AAPL [https://perma.cc/3RD4-UNAG] (last visited Jan. 24, 2021).

discussed in this Note.[56] Apple produces hardware (e.g. computers and smartphones) and software (e.g. operating systems for its devices and associated applications).[57] Its global popularity is in part due to its simple aesthetic and clean design.[58] Recently, the company refocused its brand by prioritizing user privacy, distinguishing it from other technology companies which used consumer data in their business models.[59] In the post-Snowden environment, Apple distinguished itself from companies like Google and Facebook, which rely on collecting and selling user data.[60] When Apple introduced default encryption in 2014 for its iPhones by way of iOS 8, it made a credible guarantee, backed by an algorithm, that it could not access its users' data, signifying its commitment to user privacy.[61] In addition to making encryption the default option on its devices, the company issued a public statement outlining its hardline stance on protecting the information of its consumers,[62] reaffirming that commitment with each new update of its

56. *See* Manpearl, *supra* note 20, at 160.

57. *See* CNN, *Apple, Inc.*, *supra* note 55.

58. *See* Walter Isaacson, *How Steve Jobs' Love of Simplicity Fueled a Design Revolution*, SMITHSONIAN MAG. (Sept. 2012), https://www.smithsonianmag.com/arts-culture/how-steve-jobs-love-of-simplicity-fueled-a-design-revolution-23868877/ [https://perma.cc/3RD4-UNAG]. The company founder, Steve Jobs, focused on creating a product free of the confusion and complexity commonly associated with emerging technologies. *Id.*

59. *See* Wakabayashi, *supra* note 8 ("In the iPhone's early days, Mr. Jobs told employees that the company, in effect, had a handshake agreement with customers: In exchange for buying the device, Apple would mess with their lives as little as possible, one former employee said. Generally speaking, this person said, that meant staying away from users' data and respecting their privacy.").

60. *See* Rozenshtein, *supra* note 11, at 116. By fall of 2020, Apple continued to distinguish itself from its industry competitors. Its newest smartphone operating system allows iPhone users to opt-in to companies tracking and collecting usage data across apps. *See User Privacy and Data Use*, APPLE, https://developer.apple.com/app-store/user-privacy-and-data-use/ [https://perma.cc/HN8C-BHZV] (last visited Feb. 4, 2021); Jack Nicas & Mike Isaac, *Facebook and Apple Trade Jabs*, N.Y. TIMES (Dec. 17, 2020), https://www.nytimes.com/2020/12/16/technology/facebook-takes-the-gloves-off-in-feud-with-apple.html [https://perma.cc/25WG-SQV5].

61. *See* Rozenshtein, supra note 11, at 138.

62. *See* Tim Cook, *A Message to Our Customers*, APPLE, https://www.apple.com/customer-letter [https://perma.cc/DF4D-3JGQ] (last visited Jan. 24, 2021); *see also* Romain Dillet, *Apple's Tim Cook on iPhone unlocking case*, TECHCRUNCH (Mar. 21, 2016), https://techcrunch.com/2016/03/21/apples-tim-cook-on-iphone-unlocking-case-we-will-not-shrink-from-this-responsibility/ [https://perma.cc/J9ER-Y49G] ("We have a responsibility to protect your data and your privacy. We will not shrink from this responsibility.").

operating system.[63] More, its smartphones have been at the center of prominent litigation in the United States.[64] Thus, this Note will use Apple's technology as the example moving forward.

Apple, as both a hardware manufacturer and software developer, uses both types of encryption for its smartphones. It uses a form of end-to-end encryption for its iMessage and FaceTime applications, both of which facilitate communication.[65] In addition, Apple uses device encryption to lock the entire operating system on an iPhone when not in use.[66] As an added safety measure, numerous failed password attempts reset the phone to factory settings,[67] which prevents entities from using brute-force methods to gain access to the data on the phone.[68] The company has explained that the nature of the encryption precludes it from retaining decryption keys for both forms of encryption.[69] Simply put, if decryption keys were physical items, Apple would not have a copy it could provide to law enforcement or any other entity who requests one.

Despite their supposed resistance to law enforcement requests,[70] Apple and other technology companies follow all laws of their respective jurisdictions and have issued guidance on how

63. *iOS 14 is Available Today*, APPLE (Sept. 16, 2020), https://www.apple.com/newsroom/2020/09/ios-14-is-available-today/ [https://perma.cc/C5J3-XLR6] ("More Transparency and Control with Expanded Privacy Features").

64. *See infra* Part IV.

65. *See Privacy*, APPLE, https://www.apple.com/privacy/features/ [https://perma.cc/84XP-MKZE] (last visited Jan. 24, 2021).

66. *See* Jacobsen, *supra* note 7, at 574.

67. *See* Shackelford, *supra* note 10, at 894.

68. Orin Kerr, *Preliminary thoughts on the Apple iPhone order in the San Bernardino case*, Opinion, WASH. POST (Feb. 18, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/02/18/preliminary-thoughts-on-the-apple-iphone-order-in-the-san-bernardino-case-part-1/ [https://perma.cc/3QBG-DK8K] ("I think it's probably more accurate to say that this particular model phone, the iPhone 5C, has a built-in security weakness—depending on how you define the term, a kind of backdoor—already. The government's order would require Apple to exploit the potential backdoor in Apple's design. Importantly, though, Apple redesigned its phones after the iPhone 5C to close this potential backdoor but see update below). Later phones, starting with the iPhone 5S, have apparently eliminated this potential way in. As a result, the specifics of the order in the San Bernardino case probably only involve certain older iPhones.").

69. *See* Gonzalez, *supra* note 38, at 1. For iPhone users who forget their passwords, the only solution an entire reset of the device and a complete loss of their data. *Id.*

70. *See infra* Part IV.

to request information.[71] Notably, Apple cannot extract data from passcode locked iOS devices because it "does not possess the encryption key."[72] Thus, Apple can and does make an effort to comply with law enforcement requests and is only limited by the very algorithms that fulfill its promises of privacy to consumers.

B. The Legitimate Interests of Law Enforcement

For law enforcement, the data and content on encrypted smartphones offer significant evidentiary value.[73] As one legal scholar frames it, "[t]his mass of data tells rich stories about our lives—what we do and where, when, and with whom we do it. Hence, it's a treasure trove for surveillance officials."[74] The data that can be recovered from encrypted smartphones can provide inculpatory evidence for past crimes or help prevent future ones.[75] Targeted criminal activity ranges between terrorist acts,

71. Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), https://www.apple.com/customer-letter/ [https://perma.cc/NC78-JRCF] [hereinafter Cook *Letter*]. On its website, Apple provides guidance for law enforcement both in the United States and in outside jurisdictions. For the United States, Apple "will only provide content in response to a search warrant issued upon a showing of probable cause." *Legal Process Guidelines: Government & Law Enforcement within the United States*, APPLE, https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf [https://perma.cc/ZRK3-FNUS] (last visited Jan. 24, 2020) [hereinafter Apple US Guidelines]. For jurisdictions outside the United States, Apple states that for it "to disclose customer information in response to a request from law enforcement, it is necessary for the requesting officer to indicate the legal basis which authorises the collection of evidential information in the form of personal data by a law enforcement agency from a Data Controller such as Apple." *Legal Process Guidelines: Government & Law Enforcement outside the United States*, APPLE, https://www.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf [https://perma.cc/T7RK-BZW6] (last visited Jan. 24, 2021) [hereinafter Apple Int'l Guidelines]. In any request, Apple can readily provide information on device registration, customer service records, iTunes information, retail and online store transactions, gift cards, iCloud data and content, and "Find My iPhone" data. *See* Apple US Guidelines, *supra* note 71; Apple Int'l Guidelines, *supra* note 71.

72. *See* Apple US Guidelines, *supra* note 71, at 11; Apple Int'l Guidelines, *supra* note 71, at 11; *see also* Caren Morrison, *Private Actors, Corporate Data, and National Security: What Assistance Do Tech Companies Owe Law Enforcement*, 26 WM. & MARY BILL RTS. J, 407, 410 (2017).

73. *See* CARNEGIE, *supra* note 12, at 11.

74. *See* Rozenshtein, *supra* note 11, at 114.

75. *See* Jacobsen, *supra* note 7, at 577-78; *see* Eric Manpearl, *Preventing "Going Dark": A Sober Analysis and Reasonable Solution to Preserve Security in the Encryption Debate*, 28 U. FLA. J. L. & PUB. POL'Y 65, 74 (2017) [hereinafter Manpearl II].

crimes in local areas, and the sexual exploitation of children.[76] Often, a significant amount of information can only be found on the physical smartphone (as opposed to the data being transmitted elsewhere) either because of the way the smartphone software processes the code or because the user opts in to the smartphone's protective measures, preventing the data from being accessed remotely.[77] Encryption, thus, serves as a barrier to these law enforcement interests because encryption code prevents law enforcement from accessing underlying data that may be necessary for the prevention, detection, and solution of crimes.[78] This Section will elaborate on some of these government interests and the way encryption has frustrated law enforcement efforts.

1. National Security

The September 11 terrorist attacks saw a marked shift in US government surveillance tactics starting with 2001's Patriot Act which conveyed increased surveillance powers to US law enforcement in its counterterrorism efforts.[79] Timothy Edgar, who helped build some of the surveillance programs used by the US's National Security Agency ("NSA") that were later revealed by Snowden in 2013, argues that technology-enhanced surveillance tactics have been necessary in neutralizing terrorists and other intelligence targets.[80] The data that can be recovered from encrypted smartphones belonging to suspected terrorists can be necessary, according to top US officials, in preventing

76. MANHATTAN DIST. ATTORNEY'S OFFICE, REPORT ON SMARTPHONE ENCRYPTION AND PUBLIC SAFETY i (2015), https://www.manhattanda.org/wp-content/themes/dany/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety.pdf [https://perma.cc/U5ZG-RNNN] [hereinafter Vance 2015].

77. *See* Jacobsen, *supra* note 7, at 577-78.

78. *See* PAYTON & CLAYPOOLE, *supra* note 44, at 207; Manpearl II, *supra* note 75 at 66; Morrison, *supra* note 72, at 409.

79. *See* Lee & Pearlman, *supra* note 28, at 769. The specific provision of the 2001 Patriot Act was later declared unlawful by a US court but Congress quickly followed with a replacement. *See* TIMOTHY H. EDGAR, BEYOND SNOWDEN: PRIVACY, MASS SURVEILLANCE, AND THE STRUGGLE TO REFORM THE NSA 4 (Brookings Inst. Press 2017). The concern was global, with other nations expressing similar fears of terrorist attacks, culminating in the multilateral cooperation between nations exchanging data and information in the interest of keeping those within their borders safe. *Id.*

80. *See* EDGAR, *supra* note 79, at 8.

future attacks or for gathering information on the perpetrators of a past attack.[81] The events and aftermath of two distinct terrorist attacks in the United States vindicates these national security concerns.

On December 2, 2015, Syed Rizwan Farook and Tashfeen Malik walked into a holiday party at a social services center in San Bernardino, California, and killed fourteen people while injuring twenty-one others.[82] The Islamic State, a militant terrorist group based in Iraq and Syria, quickly took credit for the attack, though there was no evidence directly linking the shooters to the group.[83] The Federal Bureau of Investigation ("FBI") recovered Farook's iPhone and with Apple's assistance was able to recover iCloud data that was backed up through October 19, leaving six weeks of data unaccounted for.[84] The FBI sought further help from Apple in extracting the remaining data, but Apple refused, explaining it would not write code that allows the FBI to bypass the phone's encryption measures.[85] The FBI sought a judgment to compel Apple to write code that would permit backdoor access to the

81. *See, e.g.*, Att'y Gen. William P. Barr, Keynote Address at the International Conference on Cyber Security 1, 5 (July 23, 2019); Lee & Pearlman, *supra* note 28, at 786; Dunlap, *supra* note 13, at 1697.

82. *See* Michael S. Schmidt & Richard Pérez-Peña, *F.B.I. Is Treating Rampage as Act of Terrorism*, N.Y. TIMES, Dec. 5, 2015, at A1, https://www.nytimes.com/2015/12/05/us/tashfeen-malik-islamic-state.html [https://perma.cc/7XJL-98TD]; Alex Dobuzinskis, *In San Bernardino, solemn ceremony marks mass shooting*, REUTERS (Dec. 2, 2016), https://www.reuters.com/article/us-california-shooting-anniversary/in-san-bernardino-solemn-ceremony-marks-mass-shooting-idUSKBN13R13R [https://perma.cc/ZV8J-XTEM].

83. *See* Laura Wagner, *Still No Evidence Linking San Bernardino Shooters to ISIS, FBI Says*, NPR (Dec. 16, 2015), https://www.npr.org/sections/thetwo-way/2015/12/16/460021165/still-no-evidence-linking-san-bernardino-shooters-to-isis-fbi-says [https://perma.cc/VAE5-ANAA].

84. *See* Ellen Nakashima & Mark Berman, *FBI asked San Bernardino to reset the password for shooter's phone backup*, WASH. POST (Feb. 20, 2016), https://www.washingtonpost.com/world/national-security/fbi-asked-san-bernardino-to-reset-the-password-for-shooters-phone-backup/2016/02/20/21fe9684-d800-11e5-be55-2cc3c1e4b76b_story.html [https://perma.cc/Q8PN-UYGJ].

85. *See* Ellen Nakashima, *Why Apple is in a historic fight with the government over one iPhone*, WASH. POST (Feb. 17, 2016), https://www.washingtonpost.com/world/national-security/why-apple-is-in-a-historic-fight-with-the-government-over-one-iphone/2016/02/17/c512c9ba-d59b-11e5-9823-02b905009f99_story.html [https://perma.cc/FZ76-QZYV]; *see* Leander Kahney, *The FBI Wanted a Back Door to the iPhone. Tim Cook Said No*, WIRED MAG. (Apr. 16, 2019), https://www.wired.com/story/the-time-tim-cook-stood-his-ground-against-fbi/ [https://perma.cc/H69Z-CH28].

phone,[86] but dropped the case a few months later after reportedly paying a third-party company over US$1.3 million to hack the phone.[87] The FBI did not reveal whether the extracted information was useful.[88]

The US government encountered this problem again more recently in January 2020 when it recovered two iPhones belonging to a suspected terrorist, and was again unable to access the iPhones' password-protected contents.[89] On December 8, 2019, Mohammed Saeed Alshamrani went on a shooting rampage at the Naval Air Station in Pensacola, Florida.[90] Apple turned over the relevant data that was in its possession, but again stated it was unable to access the data on the locked, encrypted iPhone, and that it would not write code permitting backdoor access into the device.[91] More than four months later in May 2020, the FBI managed to access the data through an alternative method,[92] and found evidence of Alshamrani's connection with al-Qaida.[93]

---

86. The case and other judicial opinions will be analyzed later on in this Note. *See infra* Part IV.

87. *See* Eric Lichtblau & Katie Benner, *F.B.I. Director Suggests Bill for an iPhone Hacking Topped $1.3 Million*, N.Y. TIMES, Apr. 22, 2016, at B3, https://www.nytimes.com/2016/04/22/us/politics/fbi-director-suggests-bill-for-iphone-hacking-was-1-3-million.html [https://perma.cc/8V4W-49K6]; Katie Benner & Eric Lichtblau, *U.S. Says It Has Unlocked an iPhone Without Apple*, N.Y. TIMES, Mar. 29, 2016, at A1, https://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html [https://perma.cc/GU6A-WKME].

88. *See* Eric Lichtblau, *F.B.I. Lawyer Won't Say If Data from Unlocked iPhone is Useful*, N.Y. TIMES, Apr. 6, 2016, at B3. https://www.nytimes.com/2016/04/06/technology/fbi-lawyer-wont-say-if-data-from-unlocked-iphone-is-useful.html?_r=0 [https://perma.cc/DMR4-6BD7].

89. *See* Shannon Bond, *Apple Declines DOJ Request to Unlock Pensacola Gunman's Phones*, NPR (Jan. 14, 2020), https://www.npr.org/2020/01/14/796160524/apple-declines-doj-request-to-unlock-pensacola-gunmans-phones [https://perma.cc/D9PE-8YMB]; Jack Nicas & Katie Benner, *F.B.I. Asks Apple To Help Unlock Two iPhones*, N.Y. TIMES, Jan. 8, 2020, at B7, https://www.nytimes.com/2020/01/07/technology/apple-fbi-iphone-encryption.html [https://perma.cc/T9P8-96GM].

90. *See* Laurel Wamsley, *FBI Is Investigating Pensacola Shooting As Terrorism*, NPR (Dec. 8, 2019), https://www.npr.org/2019/12/08/786089099/fbi-is-investigating-pensacola-shooting-as-terrorism [https://perma.cc/D46X-C2KC].

91. *See id.*; Bond, *supra* note 89.

92. *See* Kevin Collier & Cyrus Favirar, *The FBI cracked another iPhone – but it's still not happy with Apple*, NBC NEWS (May 18, 2020), https://www.nbcnews.com/tech/security/fbi-cracked-another-iphone-it-s-still-not-happy-apple-n1209506 [https://perma.cc/F2GV-VB8E].

93. Hannah Allam, *FBI: New iPhone Evidence Shows Pensacola Shooter Had Ties To Al-Qaida*, NPR (May 18, 2020), https://www.npr.org/2020/05/18/857932909/fbi-new-

In both scenarios, in response to the US government's requests to decrypt the smartphones, Apple stated it could not do so because it did not have the decryption key. Further, Apple refused to comply with requests to write code to allow for backdoor access, citing privacy and cybersecurity concerns.[94] Ultimately, in both cases, the US government used other methods to access the encrypted data, much to the chagrin of government officials who were not content with the limited solution given that its delay and expense hindered national security investigations.[95]

The US federal government is not the only government entity citing national security concerns for gaining access to data on the encrypted smartphones. After a series of terrorist attacks in 2017, the British government expressed frustration at not being able to investigate the encrypted communications of the attackers.[96] Likewise, France and Germany have been vocal about changing EU laws regarding law enforcement access to encrypted device data after suffering numerous terrorist attacks with death tolls of over 200.[97] Australia, despite having not suffered a recent terrorist attack on the scale of those in these three mentioned countries, still cites national security concerns to justify provisions in its new law that may require technology companies to provide the Australian government access to encrypted data.[98] Lastly,

iphone-evidence-shows-pensacola-shooter-had-ties-to-al-qaida [https://perma.cc/ZJ6N-Q2AD].

94. *See* Kahney, *supra* note 85.

95. *See* Collier & Favirar, *supra* note 92; Nicas & Benner, *supra* note 89.

96. *See* Mark Scott, *Britain Demands Keys to Encrypted Messaging After London Attack*, N.Y. TIMES, Mar. 28, 2017, at B5, https://www.nytimes.com/2017/03/27/technology/whatsapp-rudd-terrorists-uk-attack.html [https://perma.cc/4X5C-93FD]. Britain's home secretary, Amber Rudd, explained that the British intelligence agencies were having trouble accessing encrypted messages sent through WhatsApp. *Id.* WhatsApp uses end-to-end encryption, which is different than the encryption focused on here, but the context is still important for this Note's analysis. *See* Leo Kelion, *WhatsApp's privacy protections questioned after terror attack*, BBC NEWS (Mar. 27, 2017), https://www.bbc.com/news/technology-39405178 [https://perma.cc/XL4W-FHFY].

97. *See* Natasha Lomas, *Encryption under fire in Europe as France and Germany call for decrypt law*, TECHCRUNCH (Aug. 24, 2016), https://techcrunch.com/2016/08/24/encryption-under-fire-in-europe-as-france-and-germany-call-for-decrypt-law/ [https://perma.cc/9QP9-WKGP]; Manpearl, *supra* note 20, at 181.

98. *See* Nellie Bowles, *Did Australia Poke Hoke in Your Phone's Security?*, N.Y. TIMES, Jan. 23, 2019, at B1, https://www.nytimes.com/2019/01/22/technology/australia-

recent laws passed in China, like the Counterterrorism Law, indicate that the Chinese government places a premium on smartphone data.[99] Given that countries often look to each other to formulate domestic policies, the debate in the United States on whether national security concerns justify government access to encrypted data likely has global implications.[100]

2. Local Crimes

Accessing data-at-rest on iPhones is also an important goal for local law enforcement agencies given that the information is just as likely to be helpful in resolving crimes unrelated to national security.[101] Recovered data can reveal information on the motivations and actions of any perpetrator, not just terrorists. Cyrus Vance, the Manhattan District Attorney and a strong advocate for data access, argues that smartphone data can be used to provide probative evidence in local crimes such as murders and serious injuries.[102] To illustrate, text message exchanges that were stored only on a smartphone were key evidence the Los Angeles Police Department used to convict two parents for the death of their two-year old daughter.[103] In another case, a long-haul trucker was convicted for sexual assault and kidnapping after law enforcement officials recovered video evidence of the assault from his cell phone.[104] A third case involves the unsolved murder of a father of six, in which the only evidence was a locked iPhone 6 and a Samsung Galaxy S6 Edge that were found beside his body.[105] Though this type of evidence can be as critical to local

---

cellphone-encryption-security.html [https://perma.cc/QXH6-PK8S]. A more thorough discussion of Australian laws will be in Section III.B.

99. *See* Lorand Laskai & Adam Segal, *The Encryption Debate in China*, CARNEGIE ENDOWMENT FOR INT'L PEACE 8 (May 30, 2019).

100. *See* Ellen Nakashima & Barton Gellman, *As encryption spreads, U.S. grapples with clash between privacy, security*, WASH. POST (Apr. 10, 2015), https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html [https://perma.cc/5BFL-V3X4].

101. *See* Manpearl, *supra* note 20, at 163.

102. *See* VANCE 2016, *supra* note 16, at 8.

103. *See* Jacobsen, *supra* note 7, at 577.

104. *See* Nakashima & Gellman, *supra* note 100.

105. *See* Cyrus R. Vance Jr. et al., *When Phone Encryption Blocks Justice*, N.Y. TIMES (Aug. 11, 2015), https://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html [https://perma.cc/VA3G-VZJR].

groups in the prevention and resolution of crime, the agencies that need them are less likely to have the financial resources of the federal government to unlock the smartphones that contain them.[106] Moreover, law enforcement in smaller, local jurisdictions are more likely to encounter locked smartphones without the resources to unlock them.[107]

Other countries echo the need to use this data to solve local-level crimes. British Prime Minister David Cameron expressed, "[t]his vital communications data is absolutely crucial not just to fight terrorism but finding missing people, murder investigations."[108] Australia's Department of Home Affairs, likewise, expressed concerns on the effect that encryption has on law enforcements' ability to address organized crime, smuggling, and the sexual exploitation of children.[109] Local law enforcement agencies' need for data from encrypted smartphones is globally apparent.

3. Sexual Exploitation of Minors

Preventing the sexual exploitation of children is a special use case for decryption and stands apart from the concerns outlined above in that this interest regards a vulnerable population that the United States historically has vigorously protected.[110] A 2019 investigation by *The New York Times* revealed how child abusers and sexual predators exploit encryption technology to perpetrate their crimes.[111] Images are shared through encrypted

106. *See* Manpearl II, *supra* note 75, at 74.

107. *See id.* at 77. MANHATTAN DIST. ATTORNEY'S OFFICE, SMARTPHONE ENCRYPTION AND PUBLIC SAFETY 4-5 (2017), https://www.manhattanda.org/wp-content/themes/dany/files/2017%20Report%20of%20the%20Manhattan%20District%20Attorney%27s%20Office%20on%20Smartphone%20Encryption.pdf [https://perma.cc/5D8D-G2RD] [hereinafter VANCE 2017].

108. *See* Rowena Mason, *UK spy agencies need more powers, says Cameron*, GUARDIAN (Jan. 12, 2015), https://www.theguardian.com/uk-news/2015/jan/12/uk-spy-agencies-need-more-powers-says-cameron-paris-attacks [https://perma.cc/79ZK-XET8].

109. *See* Stilgherrian, *The Encryption Debate in Australia*, CARNEGIE ENDOWMENT FOR INT'L PEACE (2019), https://carnegieendowment.org/2019/05/30/encryption-debate-in-australia-pub-79217 [https://perma.cc/PGP6-TZLC].

110. *See Lawless Spaces: Warrant-proof Encryption and its Impact on Child Exploitation Cases*, U.S. DEP'T JUST. (Dec. 6, 2019) https://www.justice.gov/olp/lawless-spaces-warrant-proof-encryption-and-its-impact-child-exploitation-cases [https://perma.cc/U6VU-WYXP] (last updated Dec. 6, 2019).

111. *See* Michael Keller & Gabriel Dance, *The Internet Is Overrun With Images of Child Sexual Abuse. What Went Wrong?*, N.Y. TIMES (Sept. 29, 2019),

communications and stored on encrypted devices.[112] At present, technology companies report the images only when they discover them and otherwise have no legal obligation to look for them on their platforms.[113] On its products, Apple purports to use image matching technology to find images that are sent in transmission,[114] though it is unclear if that technology can be used to preemptively scan images that are stored on the phone and not sent in transmission.

US government officials frame encrypted communications and devices as a "law free zone" where predators may store images without the scrutiny of the criminal justice system.[115] To government officials, by increasing encryption options, technology companies take a step back from alleviating the

https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html [https://perma.cc/J7W3-WA28]. The piece focused on Facebook and its efforts in combatting sexual exploitation of children on its platform. Prior to switching to end-to-end encryption, Facebook actively monitored messages sent through its messaging platform and would report any child pornography to the National Center for Missing and Exploited Children. Since shifting to end-to-end encryption, its investigative mechanisms are limited by encryption because it cannot fully investigate encrypted communications for which it does not have a decryption key. That said, it continues to report images upon discovery and to develop technology that detects exploitative content. *See Community Standards: Child Sexual Exploitation, Abuse and Nudity*, FACEBOOK, https://www.facebook.com/communitystandards/child_nudity_sexual_exploitation [https://perma.cc/TFK3-BDL6] (last visited Jan. 24, 2021); Antigone Davis, *New Technology to Fight Child Exploitation*, FACEBOOK (Oct. 24, 2018), https://about.fb.com/news/2018/10/fighting-child-exploitation/ [https://perma.cc/3YZH-KX24].

112. *See* Keller & Dance, *supra* note 111; Christopher Wray, *Finding a Way Forward on Lawful Access: Bringing Child Predators out of the Shadows*, FED. BUREAU INVESTIGATION (Oct. 4, 2019), https://www.fbi.gov/news/speeches/finding-a-way-forward-on-lawful-access [https://perma.cc/86HX-SDWE].

113. *See* Keller & Dance, *supra* note 111; *see also* Katie Benner & Mike Isaac, *Child-Welfare Activists Attack Facebook Over Encryption Plans*, N.Y. TIMES (Feb. 5, 2020), https://www.nytimes.com/2020/02/05/technology/facebook-encryption-child-exploitation.html [https://perma.cc/7K6F-EKYA].

114. *See Our Commitment to Child Safety*, APPLE, https://www.apple.com/legal/child-safety/en-ww/ [https://perma.cc/3LFX-94WM] (last visited Feb. 26, 2021).

115. *See* William Barr, *Attorney General William P. Barr Delivers Remarks at the Lawful Access Summit*, U.S. DEP'T JUST. (Oct. 4, 2019), https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-remarks-lawful-access-summit [https://perma.cc/RM64-CG9D]; *see also* Dunlap, *supra* note 13, at 1698; Jacobsen, *supra* note 7, at 571 ("John J. Escalante, former Chief of Detectives for Chicago's Police Department predicts that Apple will become the phone of choice for the pedophile.") (internal citations omitted).

problem.[116] The evidence stored on smartphones could help identify victims and prevent further harms to unidentified child victims.[117] Exploitative materials can be stored on smartphones without ever being transmitted, and oftentimes, can be the only evidence of wrongdoing.[118] More, images depicting the sexual exploitation of children can cross international borders when such images are transmitted to different countries.[119] Other countries, such as Australia, are raising the alarm that encryption technology impedes efforts to tackle and end child sexual exploitation.[120] In the words of Facebook's founder, Mark Zuckerberg, "[e]ncryption is a powerful tool for privacy but that includes the privacy of people doing bad things."[121]

C. Extraordinary Access and Lawful Hacking

As explained in Section II.B above, criminal investigations are frustrated when law enforcement officials cannot access what might be potentially crucial data on an iPhone.[122] In response to the limitations created by device encryption, law enforcement agencies have pursued two technological methods, each with important legal implications. The first method, termed "extraordinary access," refers to the government, sometimes with the assistance of a technology company, accessing the data on a smartphone without external complications.[123] The second method, termed "lawful hacking," refers to exploiting existing loopholes in the software to instead hack into the smartphone.[124] The critical difference between the two, as will be explained in this Section, is that while the first method is more akin to having a skeleton key for any house, the second is more like being locked

116. *See* Barr, *supra* note 115.

117. *See* Jeffrey Rosen, *Deputy Attorney General Jeffrey A. Rosen Delivers Remarks at Justice Department's Lawful Access Summit*, U.S. DEP'T. JUST. (Oct. 4, 2019), https://www.justice.gov/opa/speech/deputy-attorney-general-jeffrey-rosen-delivers-remarks-justice-departments-lawful-access [https://perma.cc/9SCT-62EH].

118. *See* Barr, *supra* note 115.

119. *See id.*

120. *See* Julie I. Grant & Jon Rouse, *The rush to encrypt . . . and its unintended victims*, OFF. ESAFETY COMM'R (Aug. 27, 2019), https://www.esafety.gov.au/about-us/blog/rush-encryptand-its-unintended-victims [https://perma.cc/YFH4-GSFK].

121. *See* Keller & Dance, *supra* note 111.

122. *See* Kahney, *supra* note 85; discussion *supra* Section II.B.

123. *See* Levy, *supra* note 15; Bellovin, *supra* note 15, at 1.

124. *See* Levy, *supra* note 15 (reporting on lawful hacking and its implications).

out and having to pick the lock with a bobby pin or breaking a window to get inside a single house. Given this difference, two threshold issues arise: first, gaining the assistance of a technology company to create the skeleton key, and second, working around the privacy concerns raised by intruding into an otherwise private space.

Extraordinary access, sometimes called exceptional access, has been referred to as a "backdoor" for the government.[125] The access is characterized as extraordinary and exceptional because the government would only use the tool to access targeted phones as opposed to a more dragnet type of data collection.[126] Though there are several ways to accomplish this, the basic idea is to provide the government a way to access data on an encrypted smartphone without having to resort to other more intensive methods.[127] To illustrate, a government can push a software update to the targeted iPhone to remove the encryption code altogether.[128] Alternatively, a technology company can build intentional vulnerabilities into its software for all its devices to then provide special permissions to the appropriate law enforcement agencies.[129]

Backdoors provide the government with a long-term solution to the problem of encrypted smartphones because they would allow for an investigating law enforcement official to access the information without incurring additional expenses. A backdoor would have saved the FBI the US$1.3 million it reportedly spent on unlocking Syed Farook's iPhone.[130] That said, to use a backdoor, the government would need cooperation from the technology company, who would then have to alter the encryption code to provide a law enforcement official backdoor access to the phone. But, technology companies are resistant to providing the government with backdoor access that could effectively be used to decrypt any smartphone.[131] Doing so gives rise to serious cybersecurity and privacy implications because

125. *See* Traylor, *supra* note 27, at 497.
126. *See* Levy, *supra* note 15.
127. *See* Gonzalez, *supra* note 38, at 2.
128. *See* VANCE 2016, supra note 16, at 15.
129. *See id.*
130. *See* Lichtblau & Benner, *supra* note 87.
131. *See* Manpearl, *supra* note 20, at 166.

providing a backdoor weakens any encrypted ensured security.[132] Backdoors can undermine the security of encryption measures and leave smartphones vulnerable to malicious third parties like hackers or foreign nations.[133] Thus, without voluntary cooperation from the technology company, a government would have to use its existing legal framework or amend the relevant provisions to compel the company into providing the requested technical assistance.[134]

In contrast to extraordinary access, the government can use its own resources or hire a third-party to "lawfully hack" the encryption code without the technical assistance from the technology company.[135] The hacking is considered lawful because the action is authorized by the government, regardless of who ultimately does the hacking.[136] Technology companies themselves do not engage in lawful hacking because it would undermine their claims that their devices are secure.[137] Rather than installing a backdoor, lawful hacking exploits existing vulnerabilities on the phone.[138] This could mean that the hacker identifies a loophole in the encryption code that would allow him to bypass the security measures.[139] It also could refer to less complex methods by using brute-force methods and trying thousands of password combinations to gain access into the encrypted device.[140] Using the analogy above, lawful hacking can include anything from wiggling a loose doorknob until it falls off or using more forceful methods like smashing in a window to gain entry into the house.

---

132. *See id.*; Gonzalez, *supra* note 38, at 3.

133. *See* discussion *supra* Section II.A.

134. A discussion of how other countries have already amended their laws to compel backdoor access is in Part III, and a discussion of the US government's process is in Part IV.

135. *See* Manpearl II, *supra* note 75, at 83.

136. Daniel Zhang, *Revisit the Case for Lawful Hacking: A Path to the Going Dark Debate*, GEO. SEC. STUD. REV. (Dec. 13, 2019), https://georgetownsecuritystudiesreview.org/2019/12/13/revisit-the-case-for-lawful-hacking-a-path-to-the-going-dark-debate/ [https://perma.cc/W7FC-HBDT].

137. Ian Levy & Crispin Robinson, *Principles for a More Informed Exceptional Access Debate*, LAWFARE (Nov. 29, 2018), https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate [https://perma.cc/P7AB-XR27].

138. *See* Gonzalez, *supra* note 38, at 27.

139. *Id.*

140. *See* Kerr, *Preliminary thoughts*, *supra* note 68.

Unlike backdoor access, which would create a key to every phone, lawful hacking compromises only its target.[141]

Lawful hacking is a short-term solution to the problem of encrypted smartphones because a government is forced to expend time and money on a case-by-case basis.[142] Instead of having the capability of accessing every phone as it needs to, a law enforcement agency must be more selective in the phones it targets. Governments are hesitant to use lawful hacking because it often requires hiring a third-party skilled in decryption who can demand a high price tag for the service.[143] Or, if the government were to use its own resources, it may instead encounter delays on otherwise time-sensitive matters.[144] In short, what is gained by using lawful hacking—bypassing the need for cooperation from the technology company—comes with a price, and efforts are limited only to specific devices given the increased cost and longer wait times.

These complications regarding lawful hacking, consequently, limit the government from gaining access to every phone. Still, consumers rely on devices promising strong encryption measures to secure personal information from prying eyes (including those of the government). Those who value privacy as a method of control and protection from government surveillance may want to use encryption to minimize against government abuses.[145] For these individuals, lawful hacking undermines the privacy guaranteed by encryption measures, especially when the information collected from the hacking goes beyond what is reasonable. The reaction from the Snowden disclosures, for example, demonstrates that even authorized hacking can pervasively intrude upon an individual's sphere of privacy.[146] In critiquing the role of lawful hacking in the global Encryption Debate, the legal implications center more around the privacy expectations of the average user.[147]

---

141. *But see* Dunlap, *supra* note 13, at 1697.

142. *See* VANCE 2017, *supra* note 107, at 2.

143. *See* Jacobsen, *supra* note 7, at 586.

144. *See id.*

145. *See supra* Section II.A.1.

146. *See* Rozenshtein, supra note 11, at 116.

147. In the United States, this is associated with the Fourth Amendment protections. *See* Gonzalez, *supra* note 38, at 24.

This tension between encryption and legitimate government interests is global.[148] Mobile phones are ubiquitous, with a significant number of devices capable of collecting vast amounts of data about its user.[149] Apple, in particular, is one of the largest providers of smartphones with full disk encryption, and as of 2017 holds approximately thirteen percent of the global market running iOS 8 or higher.[150] In the United States, approximately forty-four percent of all mobile devices run iOS.[151] Moreover, as explained earlier, the different types of crime are not limited to one area of the world, and because of this, countries may mirror each other with the laws they ultimately enact to regulate the use of encryption.[152] Underlying the Encryption Debate is the awareness that however the debate is tackled in each country, that choice affects the global community.

III. DISCUSSION OF THE LEGAL INTERNATIONAL LANDSCAPE

Several countries have attempted to address these two issues in their respective legal frameworks. This Part focuses on the approaches adopted by the United Kingdom, Australia, Germany, and China. In addition to being the most vocal on the debate, these countries provide benchmarks on balancing the interests of law enforcement and those of technology companies and privacy advocates. The United Kingdom and Australia are members of the Five-Eyes Alliance ("FVEY")—countries that place a high value on developing tools and improving international coordination in addressing transnational crime.[153] Germany, in

148. *See* CARNEGIE, *supra* note 12, at 1.

149. JAMES A. LEWIS ET AL., THE EFFECT OF ENCRYPTION ON LAWFUL ACCESS TO COMMUNICATIONS AND DATA 18 (2017), https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/encryption/csis_study_en.pdf [https://perma.cc/A4P7-YNJM].

150. *Id.* at 8.

151. *Id.*

152. Denis McGonough, *Toward a More Constructive Encryption Debate*, CARNEGIE ENDOWMENT FOR INT'L PEACE (Apr. 25, 2019), https://carnegieendowment.org/2019/04/25/toward-more-constructive-encryption-debate-pub-79006 [https://perma.cc/VQ4N-KMB5].

153. The alliance is made up of the United States, Australia, New Zealand and Canada. FVEY is a creation of a series of formal bilateral agreements encouraging collaboration on international crime and government surveillance techniques. *See*

contrast, prioritizes user privacy above state interests. Last, China provides a unique perspective on the Debate by instead choosing to minimize the influence of technology companies and foreign states.

A. United Kingdom

The United Kingdom passed explicit laws governing law enforcement's relationship with data and encryption: the 2016 Investigatory Powers Act ("IPA")[154] and the 2018 Data Protection Act ("DPA").[155] The IPA instructs law enforcement agencies on when they can compel technology companies to facilitate encrypted data access and when they can use lawful hacking methods. The DPA, on the other hand, regulates law enforcement agencies' collection and processing of personal data. Both laws are relatively recent and UK courts have yet to fully implement either act. Thus, interpretive guidance on both laws is sparse.

1. The Investigatory Powers Act

The 2016 IPA provides the legal framework that governs a law enforcement agency's power to investigate crime.[156] The IPA was meant to consolidate existing powers into a comprehensive resource, but its passage brought out concerns about the potential for arbitrary and pervasive use.[157] The investigative methods that some provisions authorize are highly intrusive in nature and necessitate securing authorization from both the Secretary of State and an independent judge prior to their use.[158]

Rachel Taylor, *Intelligence-Sharing Agreements & International Data Protection: Avoiding A Global Surveillance State*, 17 WASH U. GLOB. STUD. L. REV. 731, 733 (2018).

154. Investigatory Powers Act 2016, c. 25 (UK).

155. Data Protection Act 2018, c. 12 (UK).

156. Confidentiality, Freedom of Information and Data Protection, P.L. Apr. 2017, 293-296 (2017).

157. Stuart MacLennan & Steve Foster, Comment, *R. (on the application of Liberty) v Secretary of State for the Home Department and Secretary of State for Foreign and Commonwealth Affairs*, 23(1) COVENTRY L. J. 105, 110 (2018); Matt Burgess, *What is the IP Act and how will it affect you?*, WIRED MAG. (May 8, 2017), https://www.wired.co.uk/article/ip-bill-law-details-passed [https://perma.cc/ZSL6-YLGV].

158. Levy & Robinson, *supra* note 137.

Further, the IPA can only be used to investigate serious crimes.[159] Serious crimes are defined to be those that carry a prison sentence of twelve months.[160] Last, the IPA sustains broad coverage and applies to foreign companies that conduct business in the United Kingdom.[161]

Section 253 of the IPA allows the government to compel technology companies to assist in accessing decrypted data.[162] Under the IPA, law enforcement agencies must secure a warrant before they can serve a technical capability notice ("TCN") on a telecommunications operator.[163] After securing the warrant, the TCN can be used to compel technology companies to remove protections on the sought data.[164] The demand for extraordinary access comes from statutory language, which imposes "obligations relating to the removal by a relevant operator of electronic protection applied by or on behalf of that operator to any communications or data."[165] Though TCNs can be deployed to compel decryption by companies who may already have encryption keys for their products, it is unclear whether they can be used to compel companies without such keys, like Apple,[166] for whom decryption would require redesigning their systems to comply with the notice.[167] Additionally, a TCN can be used to compel companies to install a "permanent interception capability" which ensures future access to encrypted data.[168] This provision has yet to be invoked.[169]

159. After being challenged in UK courts for overbroad provisions, the IPA was amended by the Data Retention and Acquisition Regulations 2018, to define serious crimes as offenses that carry a minimum of twelve months of imprisonment. The Data Retention and Acquisition Regulations 2018, SI 2018/1123 (Eng.).

160. *Id.*

161. *See* Gonzalez, *supra* note 38, at 42; Manpearl, *supra* note 20, at 206.

162. *See* Gonzalez, *supra* note 38, at 34; Manpearl, *supra* note 20, at 199.

163. Investigatory Powers Act 2016, c. 25, § 253 (UK).

164. *See* Manpearl, *supra* note 20, at 200.

165. Investigatory Powers Act 2016, c. 25, § 253(5)(c) (UK).

166. *See* Manpearl, *supra* note 20, at 201.

167. *See* Manpearl, *supra* note 20, at 200.

168. *See* Gonzalez, *supra* note 38, at 37.

169. *See* Alex Hern, *UK government can force encryption removal, but fears losing, experts say*, GUARDIAN (Mar. 29, 2017), https://www.theguardian.com/technology/2017/mar/29/uk-government-encryption-whatsapp-investigatory-powers-act [https://perma.cc/472W-MSJG].

Part 5 of the IPA authorizes "lawful hacking" by law enforcement agencies.[170] Like the requirements for extraordinary access, a law enforcement agency must secure a warrant before it can hack into the device.[171] Under this provision, the government issues targeted equipment interference warrants.[172] Warrants can be served on either the equipment owner or on an operator to assist in decrypting the data.[173] Law enforcement can use these warrants to access all types of data on a phone including communications data, speech, music, sounds, and images.[174] Unlike the TCN, equipment interference warrants can only be used on devices that law enforcement agencies reasonably believe contain information vital to national security interests or are related to the objective of investigating and solving a serious crime.[175]

To determine whether law enforcement can use either provision of the IPA, the warrant issuer must evaluate whether the government's objective in doing so is important and legitimate.[176] This is a low bar and turns on the type of crime the IPA is being used to address.[177] Once the agency passes this bar, the IPA must be implemented according to the principles of necessity and proportionality.[178] The necessity principle requires courts to consider whether there are less intrusive measures available to the government.[179] The proportionality principle requires courts to consider whether the government's proposed actions are narrowly tailored to achieve its stated goal, i.e. whether the implicated right would be limited any more than is necessary to accomplish the objective.[180] The "necessity and proportionality" analysis is meant as a procedural safeguard given the potential for government abuse.[181]

170. Investigatory Powers Act 2016, c. 25, § 5 (UK).
171. *Id.*
172. *See* Manpearl, *supra* note 20, at 203.
173. *See id.*
174. *See* Sybil Gilbert, *Someone to watch over me*, 23 COVENTRY L.J. 76, 83 (2018).
175. *See Confidentiality*, *supra* note 156.
176. *See* Gonzalez, *supra* note 38, at 39.
177. *See id.* at 38.
178. *See id.*
179. *See id.*
180. *See id.*
181. *See* MacLennan & Foster, *supra* note 157.

2. The Data Protection Act & Privacy Expectations for Mobile Data

Privacy expectations in the United Kingdom come from different sectors of the law,[182] like that in the United States.[183] In *Wainwright v Home Office*,[184] the House of Lords held that there is no general right to privacy in English common law.[185] Rather, parties seeking to make claims based on a violation of privacy must seek recourse from other legislation.[186] The Data Protection Act of 2018 is the latest piece of legislation in the UK data protection legal regime, and the primary piece of legislation used for claims alleging intrusion of privacy of personal data. Though most of the law is the United Kingdom's implementation of the EU's General Data Protection Regulation ("GDPR"), the relevant DPA provision for this Note adopts European Directive 2016/680.[187] Part 3 of the DPA dictates how law enforcement agencies collect and process data.

There are six data protection principles that must be met for a law enforcement agency to apply when processing data:

- Processing be lawful and fair;
- The purposes of processing be specified, explicit and legitimate;
- Personal data be adequate, relevant and not excessive;
- Personal data be accurate and kept up to date;
- Personal data be kept no longer than is necessary; and
- Personal data be processed in a secure manner.[188]

---

182. David Lindsay, *An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law*, 29 MELBOURNE U. L. REV. 131, 132 (2005).

183. *See infra* Part IV.

184. Wainwright v Home Office [2003] UKHL 54, [2004] 2 A.C. 406.

185. *See* N.A. Moreham, *Beyond information: physical privacy in English law*, 73(2) CAMBRIDGE L.J. 350-77 (2014).

186. *See id.* at 364. Article 8 of the 1950 European Convention for the Protection of Human Rights for example, could be used to obligate the United Kingdom to protect citizens from the misuse of data by private actors. *Id.* at 357.

187. Council Directive 2016/680, 2016 O.J. (L 119/89).

188. DEP'T FOR DIG., CULTURE MEDIA & SPORT, DATA PROT. ACT FACTSHEET (2018), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attach

Individuals whose data is being collected have rights such as: the right to knowledge of how the data is being processed; the right to rectify inaccurate data, the right to the erasure or restriction of data "where the processing of the data would infringe the data protection principles," and rights related to automated decision-making."[189] Lastly, these individuals' rights can be limited, but only where necessary and proportionate.[190]

Though the DPA is intended to be the United Kingdom's local implementation of the GDPR, the adoption of EU Directive 2016/680 through Part 3 was meant to ensure that even public officials such as law enforcement officers exercise caution in collecting and processing data.[191] The first principle, for example, recognizes that not all data collection is essential and law enforcement must show that the data could not be accessed by some other less intrusive means.[192] The third principle likewise requires that the data collected is adequate and limited to only what is necessary—the DPA does not permit a broad collection and retention of collected data.[193] Last, any data processing is subject to a "necessity and proportionality" analysis and must be applied to any law enforcement action conducted pursuant to the IPA.[194]

3. Application of the UK Legal Regime to Encrypted Smartphones

British citizens expressed displeasure about the IPA even before its passage, and referred to it as the "Snoopers' Charter" because of the expansive power given to the government to collect and investigate private and sensitive data from

ment_data/file/711215/2018-05-23_Factsheet_3_-_law_enforcement.pdf [https://perma.cc/G5JP-K9AV] (last visited Feb. 5, 2021).

189. *See id.*

190. *See id.*

191. *About the DPA 2018*, INFO. COMM'R OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/about-the-dpa-2018/ [https://perma.cc/M7NE-L99U] (last visited Jan. 24, 2021).

192. *See ICO Guide to Law Enforcement Processing*, INFO. COMM'R OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/ [https://perma.cc/C8GD-NY74] (last visited Jan. 24, 2021).

193. *See id.*

194. *See* Gonzalez, *supra* note 38, at 38.

smartphones.[195] The IPA stands starkly in contrast to the DPA, which promises a reasonable expectation of privacy from law enforcement and government surveillance. Both acts utilize a necessity and proportionality test to determine whether the access at issue is justified.

Whether it is used to secure information about a terrorist network or to gather information about a drug deal, gathering evidence in criminal investigations is an important and legitimate state objective. This objective surpasses the low threshold required by the IPA. A law enforcement agency that wants to lawfully hack into a phone must determine first whether there are less intrusive measures available to gain access. Given the amount of time and money it costs to access the phone, it is likely a warrant issuer will determine that there are no less intrusive measures available to gather the desired information. Further, these same reasons suggest that the government's proposed actions are narrowly tailored to achieve its stated goal. Lastly, the principles articulated in the DPA serve as a bulwark against overbroad searches. Law enforcement can only collect and retain essential data and must dispose of anything non-essential. Seemingly, in the United Kingdom, a citizen's reasonable expectation of privacy is protected by procedural safeguards that ensure that only relevant data is being collected and investigated.

B. Australia

Though an established member of the FVEY security and global surveillance alliance, Australia has the newest set of laws in the Encryption Debate.[196] Thus far, Australian federal law on encryption and privacy rights in the digital age is largely controlled by a single piece of legislation: the 2018 Telecommunications and Other Legislation Amendment

195. *See* Jillian Ventura, *Snoopers' Charter: Extreme Surveillance Becomes UK Law*, LAWFARE (Dec. 2, 2016), https://www.lawfareblog.com/snoopers-charter-extreme-surveillance-becomes-uk-law [https://perma.cc/259Q-BF8E]. Edward Snowden also commented on the overbroad powers given with the IPA. Edward Snowden (@Snowden), TWITTER (Nov. 4, 2015, 8:59 AM), https://twitter.com/Snowden/status/661950808381128704 [https://perma.cc/6KQS-KUZB].

196. Stilgherrian, *supra* note 109.

(Assistance and Access) Bill ("AAB").[197] The law acts similarly to the UK laws because it explicitly requires communications and service providers to develop new capabilities to intercept communications, authorizes a law enforcement agency to hack into the device, and requires foreign companies to comply when operating in Australia.[198] However, unlike the UK, Australia does not have a federal statutory scheme that protects individuals from overbroad law enforcement surveillance. Instead, that protection comes from state governments, though only one state has so-far acted in providing such protections.[199]

1. The Assistance and Access Bill

The AAB created a procedural mechanism whereby law enforcement must go through proper channels before issuing a technology capability notice on any entity that provides online services or communications equipment in Australia.[200] This law functions similarly to the UK's IPA, and evokes many of the same concerns. TCNs may compel a company to either use existing capabilities to remove electronic protection or install new capabilities to do so.[201] The type of help that a law enforcement agency can request from a technology company is outlined in Schedule 1 ("Industry Assistance") and the warrant process is explained in Schedule 2 ("Computer Access Warrants").[202] Though parts of the bill suggest otherwise, the Australian government, through the inclusion of Section 317ZG, remains

197. *See id.*

198. *See id.*

199. *See infra* note 205 and accompanying text.

200. *See* MANHATTAN DIST. ATTORNEY'S OFFICE, REPORT OF THE MANHATTAN DISTRICT ATTORNEY'S OFFICE ON SMARTPHONE ENCRYPTION AND PUBLIC SAFETY (2019), https://www.manhattanda.org/wp-content/uploads/2019/10/2019-Report-on-Smartphone-Encryption-and-Public-Safety.pdf [https://perma.cc/9NL4-RZCZ]; Kelly Buchanan, *Australia: Bill Enabling Law Enforcement and Intelligence Agencies to Access Encrypted Information Passes*, LIBR. CONG. (Dec. 14, 2018), https://www.loc.gov/law/foreign-news/article/australia-bill-enabling-law-enforcement-and-intelligence-agencies-to-access-encrypted-information-passes/ [https://perma.cc/R2KS-TUT8].

201. *See* Buchanan, *supra* note 200; Jennifer Daskal, *Privacy and Security Across Borders*, 128 YALE L.J. FORUM 1029, 1040 (2019).

202. *See Assistance and Access: Overview*, DEP'T HOME AFFAIRS, https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/assistance-and-access-overview [https://perma.cc/8UUE-YQCP] (last visited Jan. 24, 2021).

resolute that the bill cannot and will not be used to compel companies to provide extraordinary access by creating backdoors because this would undermine information security.[203] Instead, the technical assistance must be "reasonable, proportionate, practicable and technically feasible."[204] The technical assistance cannot remove existing electronic protection.[205] Additionally, the AAB can only be used on crimes that have a maximum penalty of at least three years imprisonment or more, which effectively precludes the use of the law for lesser offenses.[206] For the Australian government, compelling companies to provide technical assistance in retrieving data from smartphones is justified by the legitimate need of law enforcement to solve crime.[207] The country, however, draws the line at modifying technology such that it would weaken the security system of the device.[208]

2. Australian Expectations of Privacy

Australia does not have one comprehensive law discussing privacy—rather, like the UK, an Australian citizen's right to privacy is inferred from an amalgamation of federal, state, and territory laws.[209] The Australia federal government has not codified any protections from government surveillance, and instead such protections have come from individual states. At least two states, New South Wales and Queensland, provide some insight into how Australian law might address the issues proposed by the Encryption Debate. Given the state-based nature of privacy protections and the recency of the digital privacy legislation, it is unknown how exactly these interplay with the AAB.

---

203. *See Assistance and Access: Common myths and misconceptions*, DEP'T HOME AFFAIRS, https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/myths-assistance-access-act [https://perma.cc/7RLJ-HK6K] (last visited Jan. 24, 2021).

204. *See Assistance and Access: Overview*, *supra* note 202.

205. *Id.*

206. *Id.*

207. *Id.*

208. *Id.*

209. *See* Kelly Buchanan, *Online Privacy Law: Australia*, LIBR. CONG. (Dec. 2017), https://www.loc.gov/law/help/online-privacy-law/2017/australia.php [https://perma.cc/8R8Y-VELF].

New South Wales uses the Law Enforcement (Powers and Responsibilities) Act of 2002 ("LEPRA")[210] as the primary protection against unlawful police action. LEPRA Section 30 comes closest to addressing the search of a mobile phone during a police encounter and states in relevant part, "In conducting the search of a person, a police officer may . . . (c) examine anything in the possession of the person, and . . . (e) do any other thing authorized by this Act for the purposes of the search."[211] This provision could be interpreted to allow a police officer to search a cell phone, though it is not explicit in the text whether this type of search was contemplated by the NSW legislature when it passed the Act in 2002.

Queensland, on the other hand, has substantial statutory authority and case law elaborating when law enforcement can access data on a lawfully seized smartphone. The Police Powers and Responsibilities Act 2000 (Qld) (the "PPRA") dictates the contours of lawful searches and seizures.[212] The PPRA recognizes two types of situations necessitating lawful hacking: 1) when the perpetrator's identity is known and 2) when an unknown phone is recovered from a crime scene.[213] In both instances, the targeted phone must be linked to a crime, which provides sufficient justification to secure a warrant to hack into the phone. The PPRA discusses two types of warrants issued to allow law enforcement to access the data on a locked smartphone.[214]

Section 154 warrants are issued when the phone owner's identity is known.[215] The warrant compels the owner to provide information necessary to access the phone.[216] Failure to provide such information is a crime, the penalty for which is two to five-years imprisonment.[217] Though this raises concerns of self-

210. Law Enforcement (Powers and Responsibilities) Act, 2002 (Act No. 103.2002) (NSW) [hereinafter LEPRA].

211. *Id.* § 30.

212. Police Powers and Responsibilities Act, 2000 (Qld) §§ 5, 7 [hereinafter PPRA].

213. PPRA § 154.

214. PPRA § 178A.

215. *See* Matthew Raj & Russ Marshall, *Examining the Legitimacy of Police Power to Search Portable Electronic Devices in Queensland*, 38 U. QUEENSL. L. J. 99, 118 (2019).

216. *See id.*

217. *See id.*

incrimination, Australia does not recognize a right against self-incrimination in the way that the United States does.[218]

A Section 178A warrant is issued for phones discovered or seized from a crime scene, and where the owner's identity is unknown.[219] The warrant authorizes law enforcement to use whatever means reasonably necessary to access the data.[220] Case law on this second type of warrant is scant, but the concerns raised in case law about Section 154 warrants are just as present under this circumstance. The Supreme Court of Queensland recognized the qualitative value of iPhone evidence and advised law enforcement to exercise caution in gathering that data.[221] It was concerned with overly intrusive and pervasive government power and permitted lawful hacking provided that the law enforcement agency follows all procedures, so that lawful hacking does not raise any privacy concerns.[222]

In interpreting the PPRA, Queensland courts have cited to US Fourth Amendment caselaw. In *R v N*,[223] the Supreme Court of Queensland discussed the privacy concerns articulated in *Riley v. California*.[224] In relevant part, the Queensland Court advised exercising caution around mobile phones, saying "because of their large storage capacity and broader privacy implications, iPhones differ both quantitatively and qualitatively from other documentary records."[225] Given that the Queensland court looks to the United States for guidance on finding the balance between law enforcement interests and privacy rights, this indicates that the Australia court could come out the same way as the United States on whether lawful hacking unreasonably infringes any privacy rights. Even though the Australian federal government does not have a federal law that protects its citizens' privacy from government surveillance, at least some citizens can seek recourse in states that passed legislation to fill the gap. Thus, Queensland

218. *See* Jacobsen, *supra* note 7, at 580 ("Caselaw indicates that the government violates a defendant's Fifth Amendment right against self-incrimination when it compels the defendant to tell his numerical or alphanumerical passcode.").

219. *See* Raj & Marshall, *supra* note 215.

220. *Id.* at 119.

221. R v N [2015] QSC 91 para. 61.

222. *Id.* paras. 67-69.

223. R v N [2015] QSC 91.

224. Riley v. California, 573 U.S. 373 (2014).

225. R v N [2015] QSC 91, para. 61.

provides some insight into how other Australian jurisdictions may address lawful hacking and expectations of privacy.

C. Germany

Germany stands apart from the other countries discussed in this Note because of both its strict stance against backdoors and its more protective view of information privacy rights.[226] Germany is not representative of the European Union, nor is it the only European nation with a stake in the Debate.[227] As a leading member of the European Union, Germany was instrumental in the enactment of the GDPR, which provides broad data and privacy protections.[228] This follows from it holding itself out as a leader in encryption.[229] Germany endorses wide encryption use and encourages the development of encryption technology, despite the impediment to a law enforcement agency's ability to gain access to data.[230] The Snowden disclosures reinforced domestic views that the government had a responsibility to promote and protect infrastructures that secured the data of German citizens and companies.[231] As recently as 2017, German officials identified five guiding principles for its policy on encryption:

> 1. There will be no ban or limitation on encryption products.
>
> 2. Encryption products shall be tested for their security in order to increase the user's trust in those products.
>
> 3. The development of encryption products by German manufacturers is essential for the country's security and for

226. *See generally* Sven Herpig & Stefan Heumann, *The Encryption Debate in Germany*, CARNEGIE ENDOWMENT FOR INT'L PEACE (May 30, 2019), https://carnegieendowment.org/2019/05/30/encryption-debate-in-germany-pub-79215 [https://perma.cc/3KGL-MPAF].

227. *See* Manpearl, *supra* note 20, at 170 (discussing the Debate in France).

228. *See* Natasha Singer, *The Next Privacy Battle in Europe is Over This New Law*, N.Y. TIMES (May 27, 2018), https://www.nytimes.com/2018/05/27/technology/europe-eprivacy-regulation-battle.html [https://perma.cc/9TDB-SAL9]; Shackelford, *supra* note 10, at 905-06.

229. *See* Manpearl, *supra* note 20, at 186; *see also* Bhairav Acharya et al., *Deciphering the European Encryption Debate: Germany*, OPEN TECH. INST. 2 (Jan. 2018); *see* Herpig & Heumann, *supra* note 226, at 2.

230. *See* Manpearl, *supra* note 20, at 186 (outlining the principles); *see also* Herpig & Heumann, *supra* note 226.

231. Herpig & Heumann, *supra* note 226, at 2.

> those companies' ability to compete internationally, and shall therefore be strengthened.
>
> 4. Law enforcement and security agencies shall not be weakened by the widespread use of encryption. The development of additional technical competencies for those agencies shall be fostered.
>
> 5. International cooperation on encryption issues such as open standards and interoperability is vital and shall be fostered bi- and multilaterally.[232]

These principles suggest that though the country recognizes the need of law enforcement agencies to access that data, it will not compromise its position on encryption. Thus, discussing Germany's approach to the debate is crucial in understanding the spectrum of options from which the United States can adopt.

1. Lawful Hacking in Germany

Germany explicitly bans extraordinary access and will not compel technology companies to modify their code.[233] The country embraces encryption and permits lawful hacking methods instead.[234] There are two legal bases for law enforcement to utilize. Germany's Code of Criminal Procedure ("StPO") contains several relevant provisions: Section 100a permits law enforcement to hack devices because it facilitates the interception of communications, and Sections 94 and 98 permit hacking into lawfully seized information systems, such as smartphones.[235] The second basis is the Criminal Police Office Act ("BKAG"): Section 20k permits law enforcement officers to covertly access information systems and to collect data that is important to a case.[236] Law enforcement officers must secure a warrant from a court prior to engaging in hacking, and such warrants can only be issued for serious crimes, for example, when there is an impending danger to a person's life or for national security

232. *Id.* at 1.

233. *Id.* at 3.

234. *See* Manpearl, *supra* note 20, at 186.

235. *See* EUROPEAN PARLIAMENT POLICY DEP'T FOR CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS, LEGAL FRAMEWORKS FOR HACKING BY LAW ENFORCEMENT: IDENTIFICATION, EVALUATION, AND COMPARISON OF PRACTICES 80 (2017); Acharya et al., *supra* note 229, at 3.

236. *See* EUROPEAN PARLIAMENT, *supra* note 235.

purposes.[237] Law enforcement officers can bypass the warrant requirement if there is imminent danger of harm.[238] Last, law enforcement officers are prohibited from collecting information on "core areas" and are required to delete the information if accidentally collected.[239]

2. The Fundamental Right to Privacy

Germany's viewpoint on the Encryption Debate is largely informed by its robust protection of the fundamental right to information privacy.[240] One scholar speculates that Germany's recent history and experience as a formerly oppressive regime that engaged in massive surveillance makes the current government hesitant to implement any laws that might counteract its progress.[241] In contrast, others, including a former justice of the Federal Constitution Court (Germany's highest court), argue that the protection of fundamental rights from pervasive government intrusion predates the modern state of Germany and has always been an intrinsic part of its ethos.[242] In either case, Germany, more than the other countries discussed in this Note, places a high value on the right to privacy.

The Federal Constitution Court held on two separate occasions that overbroad lawful hacking provisions threaten the general right of personality, "which includes the fundamental right to the guarantee of the confidentiality and integrity of information technology systems."[243] In a 2008 ruling, the court struck down a provision that would have compelled technology

237. *See id.*

238. *See* Manpearl, *supra* note 20, at 189.

239. Acharya et al., *supra* note 229, at 3-4. Core areas are those that are highly private areas for the individual and includes communications between close family members and with lawyers, doctors, and the clergy. *Id.* at 4.

240. *See id.* at 2.

241. *See* Manpearl, *supra* note 20, at 192; *see also* Herpig & Heumann, *supra* note 226, at 3 ("Because of unique historical experiences with surveillance during Nazi rule and the East German Communist regime, the German intelligence community does not enjoy the positive public image that those in the United States and the United Kingdom do, and thus usually adopts a very low profile in public debates.").

242. *See* Bernhard Schlink, *Proportionality in Constitutional Law: Why Everywhere But Here?*, 22 DUKE J. COMP. & INT'L L. 291, 291 (2012); Gertrude Lübbe-Wolff, *The Principle of Proportionality in the Case-Law of the German Federal Constitutional Court*, 34 HUM. RTS. L.J. 12, 12 (2014).

243. *See* Manpearl, *supra* note 20, at 188.

companies to code backdoors in its devices because it would go against the government's responsibility to ensure the safety and integrity of its information technology systems.[244] In 2016, the Federal Constitutional Court struck down another provision finding that the present mechanisms for lawful hacking were "overly broad, lacked sufficiently independent oversight, and did not provide sufficient protections for the core area of private life."[245] The cases found that the right to privacy was a key factor in determining the outer boundaries of lawful hacking.[246] Further, in identifying that privacy was a fundamental right, the court applied the Principle of Proportionality to strike down the problematic provisions.[247]

The Principle of Proportionality demands that law enforcement powers that severely interfere with privacy must be sufficiently limited to the protection of weighty law enforcement interests.[248] The Principle of Proportionality is similar to the proportionality test applied in the United Kingdom and the balancing tests applied in Australia.[249] In applying the Principle, the Court considers three factors in its proportionality test: first, whether the act under scrutiny appropriately promotes its stated objective; second, whether it is necessary to promote that objective; and third, whether the act is adequate or proportionate in response to the need it addresses.[250]

Applying the three-factor proportionality test, German courts are likely to find that without any procedural safeguards to place a check on law enforcement agencies, lawful hacking of encrypted iPhones severely interferes with privacy rights. First, the

244. *See* Herpig & Heumann, *supra* note 226, at 6.

245. *See* Manpearl, *supra* note 20, at 189.

246. IT Federal Police Covert Surveillance Ruling, Bundes-Verfassungs-Gericht, 1BvR 966/09 ¶ 92 (Apr. 20, 2016); NRW State Police Surveillance, Bundes-Verfasungs-Gericht 1 BvR 370/07 ¶ 196-198 (Feb. 27, 2008).

247. IT Federal Police Covert Surveillance Ruling, Bundes-Verfassungs-Gericht, 1BvR 966/09 ¶ 124 (Apr. 20, 2016) (emphasizing that the principle of proportionality places strict limitations on intrusions of privacy); NRW State Police Surveillance, Bundes-Verfasungs-Gericht 1 BvR 370/07 ¶ 167 (Feb. 27, 2008).

248. IT Federal Police Covert Surveillance Ruling, Bundes-Verfassungs-Gericht, 1BvR 966/09 HN 1b (Apr. 20, 2016).

249. *Id.*; *see supra* note 213 (discussing the balancing between privacy and enforcement); *see also supra* note 178 (discussing the principle of proportionality for determining law enforcement access to personal data).

250. Lübbe-Wolff, *supra* note 242, at 13.

legal bases are appropriate in promoting its objective but risks being overbroad if the law enforcement official does not take care to sufficiently limit its use of that power when collecting data. The relevant acts permit a law enforcement agency to collect data but do not detail how that law enforcement agency would then process that data.[251] Moreover, in the two above mentioned cases brought before the Federal Constitutional Court, the Court was concerned with lack of independent oversight.[252] Use of either the StPO or the BKAG as the legal basis for hacking into an encrypted iPhone risk failing the first factor in the Principle of Proportionality. These acts fail because they do not provide sufficient details on whether there is independent oversight of the data collection and processing. The Federal Constitution Court might be more receptive to lawful hacking if the data collection were pursuant to the same oversight to which British law enforcement are subject in the DPA. Second, whether it is necessary to hack into encrypted devices depends on the circumstances of the crime at issue. The Federal Constitutional Court has indicated that the interests to protect the "life, limb, and freedom of the individual,"[253] the continued existence of the German state, and the continued existence of the human species are legitimate reasons.[254] Within this designation, many law enforcement interests are legitimate, given that a law enforcement agency's duty is the protection of its citizens. Third, whether the act in question is adequate or proportionate in response to the need also turns on the circumstances of crime. The Federal Constitutional Court might find use of the StPO or the BKAG justified for national security reasons but less so when the acts are applied to crimes of lesser degree, such as the murder of a local individual.

Though the two cases above concerned law enforcement officers addressing only national security interests, it is likely the Federal Constitutional Court will continue to apply this reasoning

251. *See What Constitutes Data Processing?*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en [https://perma.cc/Y3XL-X7VN] (last visited Feb. 26, 2021).

252. *See* Manpearl, *supra* note 20, at 189.

253. NRW State Police Surveillance, Bundes-Verfasungs-Gericht 1 BvR 370/07 HN 2 (Feb. 27, 2008).

254. *Id.*

in the future to any lawful hacking case alleging a fundamental privacy violation. Unlike the United Kingdom and Australia, German citizens retain high expectations of privacy for the data on their phones, and have consistently indicated that expectation when propounding pro-encryption polices. Thus, even within the boundaries created so far by the German legislature and judiciary, lawful hacking may not one day be a tool available to law enforcement. Like the United States, Germany considers privacy rights against government surveillance a fundamental right enshrined in its foundational laws.[255] Though there are two ways for law enforcement to lawfully hack and intercept communications at present, the decisions of the Federal Constitution Court suggest that it is hesitant to extend these powers when lawfully hacking encrypted smartphones reveals more information than to which a law enforcement agency is privy. Unlike the other jurisdictions discussed in this Note, Germany chooses privacy over national security interests.

D. China

The final jurisdiction this Note discusses is China, whose role in the Encryption Debate stands apart from the others because of the country's distinctive motivations for its use of encryption technology. The Snowden disclosures prompted its leadership to reduce the country's dependency on foreign companies.[256] China was concerned that the United States would continue to manipulate US-based technologies to surveil those within Chinese borders.[257] Hence, China's government seeks to limit the use of surveillance technology by foreign countries within its borders, which stands in contrast to its own stance on using surveillance technology on its citizens,[258] prompting some to characterize China as a surveillance state.[259] Many Chinese citizens are

255. *See* Manpearl, *supra* note 20, at 189.

256. *See* Laskai & Segal, *supra* note 99, at 1; Rozenshtein, *supra* note 11, at 117.

257. Adam Segal, *China, Encryption Policy, and International Influence*, HOOVER INST. 1 (2016), https://www.hoover.org/sites/default/files/research/docs/segal_webreadypdf_updatedfinal.pdf [https://perma.cc/QHT2-VDD4].

258. *See* Laskai & Segal, *supra* note 99, at 2.

259. Jim Baker, *Rethinking Encryption*, LAWFARE (Oct. 22, 2019), https://www.lawfareblog.com/rethinking-encryption [https://perma.cc/D98G-ZQFX].

increasingly demanding their information privacy rights,[260] a demand that has intensified as their government implements new technologies that collect private information for monitoring purposes.[261] China's actions thus far suggest two conclusions with regard to the Encryption Debate. First, that it can and has compelled technology companies to be compliant with laws requiring technical assistance to encrypted devices. Second, that lawful hacking does not implicate any existing privacy rights.

1. China's Development of Encryption Technologies

In direct response to the Snowden disclosures, the Chinese government reinitiated efforts to strengthen its cybersecurity infrastructure to withstand spying and attacks from foreign governments,[262] though its interest in encrypted information predates the disclosures.[263] China has invested heavily in developing secure encryption technologies, and tasked several government agencies to research, test, and promulgate standards for encryption related issues.[264] These efforts are aimed at developing domestic encryption technology while reducing the use and influence of foreign encryption technology,[265] resulting in several laws that impose strict obligations on foreign companies seeking to do business in China.

China, as early as 2003, required that all wireless devices sold in the country comply with the WLAN Authentication and Privacy Infrastructure ("WAPI") standard, claiming it to be more secure that others at the time.[266] Despite heavy pushback from US-based technology companies, eventually some complied, with Apple introducing iPhone models that met the WAPI standard.[267] The FBI speculated that these early models essentially came with

260. *See* Laskai & Segal, *supra* note 99, at 7.
261. *Id.*
262. *Id.* at 1.
263. *See* Segal, *supra* note 257, at 2.
264. *See* Laskai & Segal, *supra* note 99, at 3.
265. *Id.* at 4.
266. *Id.*
267. *Id.* at 5 ("Despite these setbacks, Apple and Dell both eventually introduced phone models that support Wifi and WAPI, a sign of the Chinese government's successful ability to leverage market access to shape the behavior of foreign companies"). China later discarded the mandate after facing substantial foreign pressure. *Id.* at 8.

backdoors for the Chinese government.[268] China regularly updated its laws to keep up with the change in technology, with each law reaffirming the obligation to comply with domestic encryption polices. The 2015 Counterterrorism Law,[269] for example, imposes on telecommunication operators a requirement to provide technical support and decryption services to Chinese authorities for public security and intelligence gathering purposes.[270] A previous version of the law included language that effectively imposed a backdoor requirement on all technology companies.[271] China, however, removed that language after severe criticism from the international community, including from the United States.[272]

The 2017 Cybersecurity Law[273] further requires technology companies to keep a record of users' online activities for at least six months.[274] Section 41, in particular, emphasizes that network operators, which is broadly defined to include Apple, must provide technical support and assistance during law enforcement investigations.[275] Chinese press have interpreted these provisions as comparable to the United Kingdom's IPA and Australia's AAB.[276] To comply with the Cybersecurity Law, Apple migrated its iCloud data to a local Chinese cloud service[277] and transferred the encryption keys for the cloud data to Chinese authorities.[278] Important to note, this was data to which Apple was already privy,[279] unlike data that can be recovered from end-to-end encrypted communications or from iPhones secured with device encryption. Thus, Apple's compliance here does not undermine

268. *See* Segal *supra* note 257, at 3.

269. *See generally* Zhonghua Renmin Gongheguo Fan Kongbu Zhuyi Fa [Counterterrorism Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l. People's Cong. Dec. 27, 2015, effective Jan. 1, 2016) (China).

270. *See* Manpearl, *supra* note 20, at 209; Laskai & Segal, *supra* note 99, at 8; Segal, *supra* note 257, at 5.

271. *See* Manpearl, *supra* note 20, at 209.

272. *See id.*

273. *See generally* Zhonghua Renmin Gongheguo Wangluo Anquan Fa [Cybersecurity Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Nov. 7, 2016, effective June 1, 2017) (China).

274. *See* Laskai & Segal, *supra* note 99, at 8.

275. *See* Manpearl, *supra* note 20, at 210.

276. *See* Laskai & Segal, *supra* note 99, at 2.

277. *See* Laskai & Segal, *supra* note 99, at 8; Rozenshtein, *supra* note 11, at 119 n.97.

278. *See* Laskai & Segal, *supra* note 99, at 7; *see also* Manpearl, *supra* note 20, at 214.

279. *See* Apple US Guidelines, *supra* note 71; Apple Int'l Guidelines, *supra* note 71.

its argument that it does not have a decryption key to otherwise encrypted data. Interestingly, China banned several end-to-end encrypted communication services, with the sole exception being Apple's iMessage.[280] Apple has also acquiesced to demands for app removal from the App Store, including an app that purportedly helped Hong Kong protestors target police officers and other privacy-protecting VPN apps.[281]

On October 26, 2019, China passed the newest iteration of its encryption regulatory regime, the Encryption Law.[282] The law classifies encryption uses into three categories—core encryption, ordinary encryption, and commercial encryption—and articulates that while core encryption and ordinary encryption are used for guarding safe secrets, commercial encryption is not.[283] The law does not provide a definition of what constitutes commercial encryption (leaving open the question whether consumer devices like iPhones fall into that category) though it is thought to alleviate some of the burdens imposed by previous laws.[284]

In any case, in spite of the ambiguities in China's laws on encryption, Apple's compliance thus far with Chinese laws and regulations suggests that it will not resist future efforts to regulate encryption measures, including the requirement to provide a backdoor into encrypted smartphones. Though this seems odd given that in other jurisdictions Apple has resisted such efforts, its yielding to Chinese demands is more reasonable when dealing with a market saturated with competitors capable of providing encryption capabilities on their devices.[285] Yet, even Chinese technology companies have resisted against China's requests. A Chinese ride-sharing company, for example, refused a law

280. *See* Laskai & Segal, *supra* note 99, at 8.

281. *See* Burgess, *supra* note 157.

282. People's Republic of China Encryption Law (promulgated by the Standing Comm. Nat'l People's Cong. Oct. 26, 2019, effective Jan. 1, 2020).

283. *See* Yan Luo et al., *China Enacts Encryption Law*, COVINGTON (Oct. 31, 2019), https://www.cov.com/-/media/files/corporate/publications/2019/10/china_enacts_encryption_law.pdf [https://perma.cc/J4TS-WL5M]; Samm Sacks, *Data Security and US China Tech Entanglement*, LAWFARE (Apr. 2, 2020, 8:00 AM), https://www.lawfareblog.com/data-security-and-us-china-tech-entanglement [https://perma.cc/ETW2-BLB9] (Sacks refers to the Encryption Law as the Cryptography Law. Both titles are correct.).

284. *See* Luo et al., *supra* note 283; Laskai & Segal, *supra* note 99, at 9.

285. *See* Manpearl, *supra* note 20, at 213.

enforcement request for data to be used in investigating the murder of passengers.[286] Huawei, the dominant smartphone manufacturer in China,[287] indicated it had reservations about a backdoor requirement when it expressed its support for Apple in the 2015 legal fight with the FBI.[288] Chinese internet giants, Alibaba and Tencent, pushed back against government requests for data, explaining that such interference harms their expansion into the global market.[289] Unlike its battles in other jurisdictions, Apple has the benefit of being backed by foreign nations and other dominant technology companies when pressured to comply with harsh Chinese laws.

2. China as a Surveillance State

In addition to developing domestic encryption technologies in response to perceived threats from foreign nations and companies, China's investment in domestic products arises from otherwise lacking data protection for its citizens.[290] A significant number of Chinese citizens are victims of data leaks, with their data contributing to a thriving black market.[291] China does not have a single privacy and data protection law, and like the UK, develops its privacy protections piecemeal.[292] In response to lack of data protection laws, the country in 2018 published the Personal Information Security Specification, a nonbinding standard that is meant to induce technology companies into providing stronger encryption measures on their smartphones.[293] The Cybersecurity Law, likewise, was passed in response to the threat from third parties seeking unauthorized access to

286. Sacks, *supra* note 283.

287. *See* Manpearl, *supra* note 20, at 214.

288. *See* Segal, *supra* note 257, at 9; Caroline Hyde, *China's Huawei Backs Apple Stance in Phone Unlocking Dispute*, BLOOMBERG (Feb. 21, 2016), https://www.bloomberg.com/news/articles/2016-02-22/china-s-huawei-backs-apple-stance-in-phone-unlocking-dispute [https://perma.cc/AW8Q-KAG9].

289. Samm Sacks, *China's Cybersecurity Law Takes Effect: What to Expect*, LAWFARE (June 1, 2017), https://www.lawfareblog.com/chinas-cybersecurity-law-takes-effect-what-expect [https://perma.cc/L5WU-VVKN] [hereinafter Sacks, *Cybersecurity*].

290. *See* Laskai & Segal, *supra* note 99, at 7.

291. *See id.*

292. *See* Samuel Yang, *China: Privacy*, GLOB. DATA REV. (Dec. 4, 2019), https://globaldatareview.com/insight/handbook/2021/article/china-privacy [https://perma.cc/JNT6-N7R2].

293. *See* Laskai & Segal, *supra* note 20, at 7.

consumer data.[294] Since its passage, the Cybersecurity Law serves as the government's main piece of legislation for data protection and control.[295]

Though these laws suggest China respects the privacy of its citizens, that respect does not extend to privacy from government surveillance.[296] The provisions imposing strict obligations on technology companies to assist with law enforcement investigations and efforts apply to all companies operating within Chinese borders, not just foreign ones. More, its development of a social credit system undermines any claims that it seeks to secure the privacy and confidential information of its citizens.[297]

Many consumers worldwide have experienced a variation of the social credit system: a credit score based on debt repayment, the ratings given by Uber and similar ridesharing companies, and even likes and comments received on an Instagram post.[298] The system bears an eerie resemblance to the *Black Mirror*[299] episode where individuals rank every social interaction with each other and rankings directly contribute to a person's standing in society.[300] The idea of quantifying a person's action to either reward or penalize them is not a new one, and here, once the system is fully implemented, the idea will be applied on a much larger and more formal scale.[301] At present, only some local governments have pilot programs in place, with each program

294. *See* Yang, *supra* note 292.

295. *See* Sacks, *supra* note 283.

296. *See* Segal, *supra* note 257, at 10.

297. Nicole Kobie, *The complicated truth about China's social credit system*, WIRED MAG. (June 7, 2019), https://www.wired.co.uk/article/china-social-credit-system-explained [https://perma.cc/X9RV-T7A6].

298. *Id.*

299. Black Mirror is a science fiction anthology show in which the issue of each standalone episode revolves around a piece of technology and its effects on the characters' lives. *See* NETFLIX https://www.netflix.com/title/70264888 [https://perma.cc/6LXV-FKD7] (last visited Jan. 24, 2021).

300. *Black Mirror: Nosedive*, NETFLIX (Oct. 21, 2016); Sophie Gilbert, *Black Mirror's 'Nosedive' Skewers Social Media*, ATLANTIC (Oct. 21, 2016), https://www.theatlantic.com/entertainment/archive/2016/10/black-mirror-nosedive-review-season-three-netflix/504668/ [https://perma.cc/TVJ3-YMK9].

301. *See* Kobie, *supra* note 297 ("The idea itself is not a Chinese phenomenon . . . But if the Chinese system does come together as envisioned, it would still be something very unique. It's both unique and part of a global trend.").

varying from the next.[302] One city, for example, starts all residents at 1,000 points and makes deductions for bad behavior and additions for good behavior.[303] Tracking everyday behavior is made easier with the widespread use of facial recognition technology and data sharing between companies.[304] China justifies the use of such a system to build trust, enforce laws, and hold bad actors accountable.[305] It frames the system as way to further protect its citizens from those who would maliciously use personal information and provides individuals with an alternative means of building financial credit.[306] If anything, the social credit system falls within the purview of China's goal to increase data protection for its citizens by using new technologies in its governance scheme.[307]

Between laws requiring technology companies to provide technical assistance and the increased use of surveillance schemes such as the social credit system, Chinese citizens do not have a reasonable expectation of privacy for the data on their smartphones. Law enforcement agencies can access digital communications given that encryption is virtually not allowed on most services in the country, and the robust development of encryption technology largely overcomes potential barriers in hacking the phone. Not only does China endorse lawful hacking, it actively strives to ensure access to that data. Thus, though it has concerns when other unauthorized persons gain access to its citizens' data, China itself holds carte blanche to all communications and data.

---

302. *Id.*; Louise Matsakis, *How the West Got China's Social Credit Wrong*, WIRED MAG. (July 29, 2019), https://www.wired.com/story/china-social-credit-score-system/ [https://perma.cc/9QGV-XSK9].

303. *See* Kobie, *supra* note 297; Matsakis, *supra* note 302.

304. *See* Kobie, *supra* note 297; Matsakis, *supra* note 302. Those with a deficit of social credit face restrictions on their choices and movements. Likewise, those with a positive rating gain access to discounts, benefits, and other rewards from the government. *Id.*

305. *See* Kobie, *supra* note 297; Matsakis, *supra* note 302.

306. *See* Kobie, *supra* note 297; Matsakis, *supra* note 302.

307. Eunsun Cho, *The Social Credit System: Not Just Another Chinese Idiosyncrasy*, J. PUB. & INT'L AFFAIRS, https://jpia.princeton.edu/news/social-credit-system-not-just-another-chinese-idiosyncrasy [https://perma.cc/GY9N-ZR3Y] (last visited Jan. 24, 2021).

IV. UNITED STATES

The Encryption Debate in the United States is arguably the most notable of all the countries discussed in this Note, primarily because of the divisive split in public opinion when the US government first requested a court order to compel Apple to assist FBI agents in accessing the data on a suspected terrorist's phone.[308] The debate at the time largely focused on the first issue, whether the US government could use the All Writs Act ("AWA")[309] to compel a technology company like Apple to build a backdoor into its smartphone. Within two weeks of each other, two separate federal courts issued contradictory orders on the limits of the AWA as applied to the circumstances of this Debate.[310] US courts throughout the country have entertained several similar suits, yet none have made it to the Supreme Court.[311] In addition to the concerns raised by the first issue, some commentators have speculated about whether the Fourth Amendment limits the government from hacking into an encrypted smartphone.[312] Unlike the first issue, the Supreme

308. *See* Krisnadev Calamur, *Public Opinion Supports Apple Over the FBI—or Does It?*, ATLANTIC (Feb. 24, 2016), https://www.theatlantic.com/national/archive/2016/02/apple-fbi-polls/470736/ [https://perma.cc/BD42-U2W2]; Dustin Volz & Abhirup Roy, *U.S. government, Apple take encryption case to court of public opinion*, REUTERS (Feb. 22, 2016), https://www.reuters.com/article/us-apple-encryption-commission/u-s-government-apple-take-encryption-case-to-court-of-public-opinion-idUSKCN0VV185 [https://perma.cc/68NB-4SHE]; Tracey Lien, *Whether Apple or FBI is winning the PR war depends on which poll you're looking at*, L.A. TIMES (Feb. 24, 2016), https://www.latimes.com/business/technology/la-fi-tn-apple-fbi-polls-20160224-story.html. The case drew considerable attention from technology moguls and advocates. *See Amicus Briefs in Support of Apple*, APPLE (Mar. 2, 2016), https://www.apple.com/newsroom/2016/03/03Amicus-Briefs-in-Support-of-Apple/ [https://perma.cc/3VGT-8P8A]; Jacobsen, *supra* note 7, at 569.

309. All Writs Act, 28 U.S.C. § 1651(2018).

310. *See infra* Section IV.A.

311. *See, e.g.*, *In re:* Order Requiring Apple, Inc. to Assist in The Execution of a Search Warrant Issued by this Court, 149 F. Supp. 3d 341, 349 (E.D.N.Y. 2016) [hereinafter *Brooklyn action*]. At the time of the *Brooklyn action*, there were at least nine separate requests made under the AWA to order Apple to help the government with bypassing the encryption measures—Apple objected to each request. *Id.* at 349.

312. *See* Grady Lowman, *Apple vs. FBI: The Forgotten Fourth Amendment Argument*, RUTGERS J. L. & PUB. POL'Y (Mar. 21, 2016), https://rutgerspolicyjournal.org/apple-vs-fbi-forgotten-fourth-amendment-argument [https://perma.cc/RM6Q-4UUN]; Maxel Moreland, *Apple Inc. and the FBI: Balancing Fourth Amendment Privacy Concerns against Societal Safety Concerns in the Digital Age*, U. CIN. L. REV. (June 17, 2016), https://uclawreview.org/2016/06/17/apple-inc-and-the-fbi-balancing-4th-amendment-

Court has discussed, as recently as 2018, the Fourth Amendment's relationship with data from smartphones.[313] Regarding the second issue, whether lawful hacking violates reasonable expectations of privacy, recent Fourth Amendment decisions about cell phones suggest that cell phone data must be given heightened protection.[314] This Part will proceed by first, offering a discussion on the AWA by analyzing the first issue, and then second, by discussing the Fourth Amendment and analyzing the second issue.

A. Using the All Writs Act to Compel Apple to Create a Backdoor for the US Government

The All Writs Act states that "[t]he Supreme Court and all courts established by Act of Congress may issue all writs necessary and appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."[315] The act serves as a gap-filler for a federal court to use when no other law might provide it authority to make a judgment or an order.[316] As a threshold matter, federal courts are only given discretionary authority to issue orders when three elements are met:

> (1) issuance of the writ must be 'in aid of' the issuing court's jurisdiction;
>
> (2) the type of writ requested must be necessary or appropriate to provide such aid to the issuing court's jurisdiction; and
>
> (3) the issuance of the writ must be agreeable to the usages and principles of law.[317]

However, the All Writs Act is infrequently used, and there is little judicial guidance on whether it could be used to compel Apple to modify its code to provide a backdoor into its devices.[318]

---

privacy-concerns-against-societal-safety-concerns-in-the-digital-age/ [https://perma.cc/CE96-SDFM]. *But see* Kerr, *Preliminary thoughts, supra* note 68; Traylor, *supra* note 27, at 510.

313. *See generally* Carpenter v. United States, 138 S. Ct. 2206 (2018).

314. *See id.* at 2218.

315. All Writs Act, 28 USC § 1651 (2018).

316. *See Brooklyn action*, 149 F. Supp. 3d at 353.

317. *Id.* at 350.

318. *See id.* at 349.

The most recent Supreme Court decision involving AWA, *United States v. New York Telephone Co.*,[319] offers some guidance for how to interpret the act. It was a different time with different technologies, yet the Supreme Court dealt with the same tension of whether the AWA could be used to compel a company to provide technical assistance to the FBI in the pursuit of shutting down criminal activities.[320] In *New York Telephone*, the FBI sought the company's help with installing pen registers[321] on phone lines belonging to individuals suspected of running a gambling ring.[322] The company, pursuant to a judicial order, had already provided some help, including identifying the telephone lines associated with the suspected phone numbers, but declined when asked to lease to the FBI unused telephone lines that ran near the suspected telephone line.[323] In finding for the FBI, the Supreme Court identified three additional factors to consider when interpreting the AWA:

> (1) the closeness of the relationship between the person or entity to whom the proposed writ is directed and the matter over which the court has jurisdiction;
>
> (2) the reasonableness of the burden to be imposed on the writ's subject; and
>
> (3) the necessity of the requested writ to aid the court's jurisdiction.[324]

So here, it was New York Telephone's facilities that were being used, the burden to lease the lines to install pen registers was very low (especially because the company itself used them for its own purposes), and it was only the company that impeded the FBI from identifying those involved in the gambling enterprise. This decision guides current understanding on the proper application of the AWA.

---

319. United States v. N.Y. Tel. Co., 434 U.S. 159 (1977).

320. *See id.* at 161.

321. Pen registers are devices that record the numbers dialed from a wired telephone. *See Pen Register*, MERRIAM-WEBSTER DICTIONARY (11th ed. 2003).

322. *See* N.Y. Tel. Co., 434 U.S. at 162.

323. *See id.* Installing a pen register on the nearby lines allowed for the FBI to monitor the incoming and outgoing calls of the suspect phone lines.

324. *See id.* at 174-78; *Brooklyn action*, 149 F. Supp. 3d. at 351.

1. Current Jurisprudence on Applying the AWA to iPhones

There is no existing explicit law that the US government can use to require a technology company to build a backdoor into its encrypted devices. When the issue was brought to court, the government depended on the AWA as its primary argument. Two different federal courts issued contemporaneous orders on whether the federal government can compel Apple to modify its encryption code to allow for extraordinary access to iPhones.[325] In both cases, the US government argued that the AWA must be interpreted to permit the government to compel Apple to assist its efforts in gathering the data from the phone.[326] In both cases, Apple argued that the AWA must be read to leave the decision to compel to the legislature.[327] Ultimately, the US government withdrew both suits, rendering the debate in the courts moot. Despite the pause in the courts, it is worth exploring these opinions to understand how the Encryption Debate could be resolved in the US given that the tension between the two entities remains.[328]

After Apple denied additional help for unlocking the iPhone recovered from the San Bernardino shooting,[329] the US Department of Justice ("DOJ") then sought the assistance of a federal court to compel the company to provide the technical assistance required.[330] Using the AWA as authority, the government argued that 1) Apple was not far removed from the underlying controversy and the related investigation because it designed the phone and coded the software at issue;[331] 2) the specific technical assistance sought would not present an unreasonable burden on Apple because a software company is

325. *See* In re: An Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, 2016 U.S. Dist. LEXIS 20543, at *1 (C.D. Cal. Feb. 17, 2016) [hereinafter *California action*]; *Brooklyn action*, 149 F. Supp. 3d. at 344.

326. *See* Govt's *Ex Parte* Appl. for Order Compelling Apple, Inc. to Assist Agents in Search; Mem. of Points and Authorities; Decl. of Christopher Pluhar; Exhibit (ED No. 15-0415M) [hereinafter *DOJ Motion*].

327. *See* Apple Inc.'s Mot. to Vacate Order Compelling Apple, Inc. to Assist Agents in Search, and Opp'n to Gov't's Mot. to Compel Assistance (ED No. CM 16-10 (SP)) [hereinafter *Apple Motion*].

328. *See supra* Section II.B.

329. *See supra* Section II.B.i.

330. *See DOJ Motion supra* note 326, at 1.

331. *See id.* at 13.

capable of modifying its own code for a specific device;[332] and 3) Apple's technical assistance is necessary in furtherance of the lawful warrant to search the phone.[333] Shortly after filing in federal court, the judge issued a three-page order requiring Apple to provide the technical assistance in the manner requested to achieve the objectives listed.[334]

Apple, in response, filed a motion to vacate the DOJ's motion, framing the DOJ's request to "create a back door" as one that would "undermine the basic security and privacy interests of hundreds of millions of individuals around the globe."[335] Apple first argues that both Congress and the Obama Administration considered the tension, and ultimately decided to not update existing relevant laws to include Apple and like technology companies within the statutory purview.[336] Next, in applying the *New York Telephone* discretionary factors, Apple argued 1) its connection to the underlying controversy and the related investigation is too attenuated because it does not own the phone nor have access to the data;[337] 2) the government's request would impose a substantial undue burden on both Apple and the customers who depend on their device;[338] and 3) the government did not establish that Apple's assistance was necessary in furtherance of the warrant.[339] A hearing was scheduled for March 22, 2016 but was later cancelled when the FBI revealed it was able to access the phone through the assistance of a third party.[340]

---

332. *See id.* at 14.

333. *See id.* at 16. The motion does not state why Apple's assistance is necessary other than citing an analogous case involving an encrypted laptop.

334. *See California action*, 2016 U.S. Dist. LEXIS 20543. Given that it was an order, there is no analysis of the AWA.

335. *See Apple Motion*, *supra* note 327, at 1.

336. *See id.* at 8.

337. *See id.* at 20.

338. *See id.* at 23.

339. *Id.* at 29. Apple also put forth arguments that the order violates its First Amendment right from writing code and its Fifth Amendment right of due process. *See generally id.* While both these arguments are important, they will not be discussed in this analysis given that this Section focuses on the use of the AWA.

340. *See* Kim Zetter & Brian Barrett, *Apple to FBI: You Can't Force Us to Hack the San Bernardino iPhone*, WIRED MAG. (Feb. 25, 2016), https://www.wired.com/2016/02/apple-brief-fbi-response-iphone/ [https://perma.cc/SPM8-V2HB]; Collier & Favirar, *supra* note 92 (reporting that the US government enlisted third-party company, Cellebrite, to hack into the phone).

In a different case, a federal judge in the Eastern District of New York entertained the same arguments as above and instead found Apple's argument to be more compelling. In *In re: Order Requiring Apple, Inc. To Assist in the Execution of a Search Warrant Issued by this Court*, the US Drug Enforcement Agency ("DEA") seized, pursuant to a warrant, an iPhone 5s running iOS7 that belonged to an individual suspected of drug trafficking.[341] As with the iPhone in California, government investigative efforts were impeded by the iPhone's passcode security.[342] The government then turned to the court to compel Apple to provide technical assistance in unlocking the phone, relying on the AWA and the cases interpreting it.[343] Finding for Apple, Judge Orenstein opined that the government failed to establish the threshold requirement that its request was agreeable to the usages and principles of law because the legislative scheme regarding the relationship between government surveillance and third-party technology and communications suggested otherwise.[344] First, the limitation provisions in the Communications Assistance for Law Enforcement Act ("CALEA")[345] apply to Apple because it qualifies under the "information services" exemption.[346] Second, issuing in favor of the government would violate the separation of powers doctrine because Congress had considered this issue and chose not to enact a law addressing it.[347] For Orenstein, the AWA analysis ends at the threshold level, but he opines on the *New York Telephone* discretionary factors to explain that the AWA analysis would still achieve the same result.[348] In sum, Apple was not sufficiently close in relationship with either the criminal activity

341. *See Brooklyn action*, 149 F. Supp. 3d 341, 345 (E.D.N.Y. 2016). Though not relevant for the purposes of the analysis, this iPhone runs an older version of iOS that has markedly less encryption measures than the iPhone from San Bernardino.

342. *See id.* at 346.

343. *See id.*

344. *See id.* at 354.

345. Communications Assistance for Law Enforcement Act, 47 U.S.C. §§ 1001-1010 (2018).

346. See *Brooklyn action*, 149 F. Supp. 3d at 355. Interestingly, Judge Orenstein accepted the distinction between data-in-motion and data-at-rest. *See supra* Section II.A. But he did not think this distinction changed his opinion that CALEA, which uses language referring to data-in-motion, applies to data-at-rest. *Id.*

347. *See id.* at 363. For a brief discussion on pending legislative actions, see Section V.A.

348. *See id.* at 364.

or the investigation,[349] compelling Apple to provide technical assistance that would erode the iPhone's encryption measures would be unduly burdensome,[350] and the availability of third parties who can provide assistance into accessing the iPhone weakens the government's argument that Apple must be the one to provide technical assistance.[351] The opinion ends by reiterating that the debate is a decision best left to be resolved by Congress.[352]

2. The All Writs Act Cannot be Interpreted to Compel Apple to Write Code that Creates a Backdoor for the Government.

Setting aside the threshold issue of whether CALEA applies and precludes this inquiry, Apple presents the stronger argument against the adoption of backdoors. The first factor, looking at the closeness of the relationship between the directed entity and the underlying controversy, favors Apple. Arguably, since it originally made the argument in 2015, Apple has provided more complex encryption measures that are less susceptible to hacking.[353] These increased measures suggest that although before Apple may not have had as close a relationship with any of the underlying crimes (indeed it did not with either the shooting or the drug trafficking), its actions have since reluctantly provided protection to those perpetrators who rely on the encryption to continue their crimes. Encrypted iPhones can now safely serve as the phone of choice for those who need that privacy measure in evading lawful governmental action. Terrorist cells can exploit the availability of encryption measures as ISIS did when it instructed its followers to use encryption measures to dodge law enforcement officials.[354] Manhattan District Attorney Cyrus Vance testified to Congress about a sex-trafficking investigation impeded by encryption, where the incarcerated suspect in a recorded phone call said, "Apple and Google came out with these softwares that can no longer be [un]encrypted by the police . . . [i]f our phone[s are]

349. *See id.*

350. *See id.* at 368.

351. *See id.* at 373.

352. *See id.* at 376.

353. The latest version of the software, iOS 14, now requires applications downloaded from the App Store to abide by Apple's privacy and security standards. *See User Privacy and Data Use*, APPLE, https://developer.apple.com/app-store/user-privacy-and-data-use/ [https://perma.cc/CZ5V-W8EQ] (last visited Jan. 24, 2021).

354. *See* Jacobsen, *supra* note 7, at 571.

running on iOS8 software, they can't open my phone. That may be [a] gift from God."[355] Last, as articulated earlier in this Note, there is an increasing concern that encryption creates a safe haven for pedophiles and others who seek to sexually exploit minors.[356] Still, these examples only serve to illustrate that while encryption may be another tool for individuals to exploit, it is simply that—a tool. The use of an iPhone in a criminal undertaking does not automatically implicate Apple, especially because there exist legitimate uses for the device and the encryption measures ensure the security of the information on the phone for the average user, not just criminal users. For comparison, if the iPhone were a gun, the blame for a shooting shifts to the person who pulled the trigger, not the gun manufacturer.[357]

The second factor, regarding the reasonableness of the burden on Apple, also is in its favor. In the California case, Apple explained the time and costs it would take to build the type of software the government seeks.[358] Critics are justifiably skeptical of this reasoning, given that Apple's market value was well over US$2 trillion in August 2020, and its products continue to see incredible success globally as society increasingly relies on technology for everyday life.[359] Apple also posited that given its role in consumer data protection, creating a system that could be

355. *See Smartphone Encryption and Public Safety: Hearing Before the S. Comm. On the Judiciary,* 116th Cong. (2019) (written testimony of Cyrus Vance, Jr., NY Cnty. Dist. Att'y), https://www.judiciary.senate.gov/imo/media/doc/Vance%20Testimony.pdf [https://perma.cc/5CNB-GH5Q].

356. *See supra* Section II.B.iii.

357. Recognizing the harm that could be imposed on firearms manufacturers, Congress effectively immunized them with the Protection of Lawful Commerce in Arms Act ("PLCAA"). *See* Protection of Lawful Commerce in Arms Act, 15 U.S.C. §§ 7901-7903; *see also* Melissa Chan, *Just About Everyone but the Gun Maker Gets Sued After a Mass Shooting*, TIME (Aug. 20, 2019), https://time.com/5653066/mass-shooting-lawsuits/ [https://perma.cc/LK7B-WJBU].

358. *See Apple motion*, *supra* note 335, at 23.

359. *See* Amrith Ramkumar, *Apple Hits $2 Trillion Market Value as App Store Battles Continue*, WALL ST. J. (Aug, 19, 2020), https://www.wsj.com/articles/apple-surges-to-2-trillion-market-value-11597848808 [https://perma.cc/9RJG-PXQV]; Jack Nicas, *Apple Reaches $2 Trillion, Punctuating Big Tech's Grip*, N.Y. TIMES (Aug. 19, 2020), https://www.nytimes.com/2020/08/19/technology/apple-2-trillion.html [https://perma.cc/XBL3-PZPD]. Almost certainly the COVID-19 pandemic benefited Apple as the shift to working from home may have led to an increased demand for the requisite technology.

vulnerable to outside attacks would "substantially tarnish the Apple brand,"[360] and would hurt the US economy overall as the subset of consumers who desire encryption shift to foreign manufacturers who sell encrypted devices.[361] Again, it is dubious whether that reasoning is valid because of the question of whether consumers actually care about data protection measures on their phone.[362] More, it is unlikely that Apple's market power would suffer at all if the US government were to institute an extraordinary access requirement.[363] Even so, the factor is likely to be in Apple's favor considering that the scale of the burden is substantially more than what the Supreme Court considered in *New York Telephone*. There, the Supreme Court found the order appropriate given that the company's own use of pen registers for business reasons demonstrated the minimal burden the FBI's request imposed upon them.[364] Unlike that of the telephone company, Apple's response would certainly cost significantly more in both time, expense, and reputation even if it is a technology giant more equipped to handle such costs.

The last factor, whether Apple's assistance is necessary to accomplish the goal of the writ, is decidedly in its favor. As Judge Orenstein astutely pointed out, the government ultimately engaging with third party companies demonstrates that Apple's technical assistance is not necessary.[365] It is true that Apple is the only actor that can modify the encryption code on its future phones, especially considering that its software is proprietary code that is installed on patented devices. Only in that sense can their assistance be necessary. But that is not the case here, because the underlying goal of a warrant issued in a criminal investigation is the resolution of a past crime or the prevention of a likely future crime, and the warrant is tied to the specific circumstances of each case.[366] Speculating on future misuse of an encrypted

360. *See Brooklyn action*, 149 F. Supp. 3d 341, 369 (E.D.N.Y. 2016).

361. *See* Manpearl, *supra* note 20, at 169-70.

362. *See* Rozenshtein, *supra* note 11, at 172.

363. *See* Manpearl, *supra* note 20, at 227.

364. United States v. N.Y. Tel. Co., 434 U.S. 159, 174 (1977) ("The Company concedes that it regularly employs such devices without court order for the purposes of checking billing operations, detecting fraud, and preventing violations of law.").

365. *See Brooklyn action*, 149 F. Supp. 3d 341 at 373.

366. *See* Marron v. United States, 275 U.S. 192, 196 (1927) ("The requirement that warrants shall particularly describe the things to be seized makes general searches under

smartphone is not a sufficient reason to characterize Apple's technical assistance as necessary. Evidently, the US federal government is equipped to either hack into the phone on its own or contract with a third party.[367]

B. The Fourth Amendment Privacy Implications of Lawful Hacking

Privacy concerns, especially privacy from government surveillance, became relevant in the Encryption Debate when Apple framed itself as a protector of its consumers' privacy.[368] To reiterate, privacy concerns are very different from the cybersecurity concerns that Apple emphasized in its motions.[369] Whereas cybersecurity touches more on the security of the infrastructure protecting the information, privacy refers more to the conception that a person has a right to be free from outside intrusion into the most intimate or confidential part of their lives.[370] Apple, in its public role as a protector of consumer data, makes good on its promise of privacy through the encryption measures on its devices.[371] The United States does not have an overall privacy law, and instead takes a sectoral approach to the right of privacy.[372] In the United States, concerns regarding privacy from government action implicate the Fourth Amendment, and this next Section will delve into whether any concerns are raised when the US government lawfully hacks into an iPhone.

1. Fourth Amendment Jurisprudence

The Fourth Amendment protects "the right of the people to be secure in their persons, houses, papers, and effects, against

---

them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken nothing is left to the discretion of the officer executing the warrant.").

367. *See* discussion *supra* Section II.B.i (explaining how the FBI hired a third party for the San Bernardino iPhone and internal methods for the Pensacola iPhones).

368. *See* Cook letter, *supra* note 71.

369. *See supra* Section II.A.i (distinguishing between privacy and cybersecurity concerns).

370. *See* Griswold v. Connecticut, 381 U.S. 479, 484 (1965) (stating that the US Constitution creates zones, or penumbras, of privacy).

371. *See supra* Section II.A.iii.

372. Ari E. Waldman, *Privacy, Notice, and Design*, 21 STAN. TECH. L. REV. 129, 144 (2018).

unreasonable searches and seizures."[373] For a search or seizure to be reasonable, a neutral judge must first issue a warrant justified by probable cause.[374] The Fourth Amendment was the Founding Fathers' response to Great Britain's arbitrary use of writs of assistance in colonial America, and imposed a limit on the federal government's ability to intrude into an individual's private physical space.[375] Though the case law has considerably changed since its adoption, the heart of the Fourth Amendment is its fundamental protection against overly pervasive government intrusion and surveillance.[376] In *Katz v. United States*,[377] the Supreme Court reframed the scope of the Fourth Amendment as a protection that is based on a person's notion of privacy, and rejected earlier interpretations that focused only on tangible, material interests.[378] The *Katz* Court found the government's use of wiretapping technology to record an otherwise private phone conversation problematic because "the Fourth Amendment protects people, not places."[379] Moving forward, the Court's Fourth Amendment analysis hinged on two-prongs: "first, that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as reasonable."[380]

Since *Katz*, the Supreme Court (and the judiciary, in general) has struggled with drawing bright-lines for which circumstances generate an objectively reasonable expectation of

373. U.S. CONST. amend. IV.

374. *Id.*

375. *See* Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018); Riley v. California, 134 S. Ct. 2473, 2494 (2014).

376. *Carpenter*, 138 S. Ct. at 2214.

377. Katz v. United States, 389 U.S. 347 (1967).

378. The majority opinion departs from the narrow view articulated in Olmstead v. United States, 277 U.S. 438 (1928), which uses the trespass doctrine to define the scope of the Fourth Amendment. *Katz*, 389 U.S. at 352. The *Katz* Court found significant the difference between the petitioner's physical presence in a public phone booth and his phone call within that space. *Id.* at 511.

379. *Katz*, 389 U.S. at 351.

380. *Id.* at 361. Even though this test is from the concurrence, it is the one that's used most often. The Court reiterated the "reasonable expectation of society" test in Rakas v. Illinois, 439 U.S. 128 (1978) (holding a party must exhibit a legitimate expectation of privacy in the place searched to have standing challenging a government search). The test was, shortly thereafter, formally adopted in Smith v. Maryland, 442 U.S. 735 (1979).

privacy,[381] especially in light of rapidly evolving technology that can undermine such expectations.[382] Yet, though the Court has identified specific circumstances that "render a warrantless search or seizure reasonable," no government action is "beyond Fourth Amendment scrutiny, for it must be reasonable in its scope and manner of execution."[383] In applying Fourth Amendment principles to its treatment of phones, two recent Supreme Court decisions are informative and touch on the heightened protections given to smartphones because, like many technologies, they have become an essential part of an individual's life. These two cases, amongst others, offers some guidance on how the Supreme Court might decide if the question of lawful hacking comes before them.

In *Riley v. California*,[384] the Court held that a warrantless search and seizure of the digital contents of a cell phone is unconstitutional, even when the phone is seized incident to an arrest. During the arrest for an earlier unlawful activity, a police officer searched David Riley and seized a smart phone from his body.[385] At that time and later again at the police station, a police officer had gone through the phone and uncovered evidence of Riley's involvement with a shooting a few weeks earlier—the investigating officers did not have a separate warrant to go through Riley's phone.[386] Chief Justice Roberts posited two observations that persuaded him and the rest of the Court that smartphones must be given special treatment. First, cell phones are ubiquitous such that an alien species may perceive it "an important feature of human anatomy."[387] Second, there is an understanding that "modern cell phones, as a category, implicate privacy concerns far beyond those implicated by a cigarette pack,

381. It is relevant to note that courts do not dwell on whether the first prong is ever met, and that the Fourth Amendment test focuses on the second prong. *See* Kerr, *supra* note 68; Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J. L. & TECH. 357, 372 (2019) [hereinafter Ohm II].

382. *See* United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

383. Maryland v. King, 569 U.S. 435, 444, 447-48 (2013).

384. Riley v. California, 573 U.S. 373 (2014).

385. *Id.* at 379. David Riley was arrested after an earlier lawful search of his car revealed his unlawful possession of concealed and loaded firearms. *Id.* at 378.

386. *Id.*

387. *Id.* at 385.

a wallet, or a purse."[388] Even a brief search through an iPhone can reveal a host of confidential information to which a person is otherwise not privy. Thus, any search for digital information on a smartphone must be done pursuant to a warrant.[389]

Carpenter v. United States[390] likewise dealt with the amount of data that can be garnered from a cell phone, more specifically, holding that law enforcement would need warrants to gather cellular service location information ("CSLI").[391] In addition to reformulating the third-party doctrine,[392] Chief Justice Roberts stressed the role of the court to rebalance privacy interests when faced against law enforcement equipped with powerful surveillance tools.[393] This decision, along with Justice Sonia Sotomayor's concurrence in *United States v. Jones*[394] and the majority opinion in *Riley*,[395] emphasizes the unique role that mobile phones play in individuals' lives and the way that technological advances give the government more tools to intrude into a person's private area.[396] Thus, investigations into smartphone data must have heightened protections.

---

388. *Id.* at 393.

389. *Id.* at 401.

390. Carpenter v. United States, 138 S.Ct. 2206 (2018).

391. *Id.* at 2223.

392. Unlike *Riley*'s inquiry into data gathered from within the device, Carpenter dealt with information collected from cell site towers and its implications for the third-party doctrine. The third-party doctrine is premised on the theory that the disclosing party adopts an assumption of risk of the further dissemination of that information by the third-party. *See* Smith v. Maryland, 442 U.S. 735, 744 (1979) (finding no reasonable expectation of privacy in pen records because the information was being conveyed to a telephone company); United States v. Miller, 425 U.S. 435, 443 (1976) (finding no reasonable expectation of privacy in bank records because this was information disclosed to banks and their employees in the ordinary course of business). Third-party doctrine is not at issue in any encryption cases because encryption ensures that the information is never disclosed to a third party. *See* Gonzalez, *supra* note 38, at 26.

393. The opinion states, in relevant part, "[f]irst, that the Amendment seeks to secure the privacies of life against arbitrary power, and Second, and relatedly, that a central aim of the Framers was to place obstacles in the way of a too permeating police surveillance." *Carpenter*, 138 S. Ct. at 2214 (citations omitted).

394. *See* United States v. Jones, 565 U.S. 400, 413 (2012).

395. *See* Riley v. California, 573 U.S. 373 (2014).

396. This is not a new view in the court. In an earlier case, Justice Kennedy opined, "[c]ell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification." *See* City of Ontario, Cal., v. Quon, 560 U.S. 746, 760 (2010).

2. Reasonable Expectations of Privacy after *Carpenter*

At present, there is no legal authority that explicitly permits lawfully hacking into encrypted devices, nor has there been any cases challenging its constitutionality.[397] Still, it stands to reason that after *Riley* and *Carpenter*, law enforcement may lawfully hack into an encrypted smartphone provided they have a warrant in hand, which is often the case. Though smartphones and smartphone data receive heightened protection, law enforcement could still access the data after securing a legitimate warrant based on probable cause. While these phones relied on encryption, a phone holder's expectation of privacy, premised on that reliance, is diminished once that device is lawfully seized and a warrant to search the contents of the phone is issued. The Fourth Amendment does not protect cell phone data *per se*, but it does protect individuals against oppressive methods in acquiring that information. The Amendment is a promise against the arbitrary use of state power. Lawfully hacking into a phone after securing a legitimate warrant does not implicate the privacy concerns raised by the Fourth Amendment.

Professor Orin Kerr has consistently argued that encryption does not trigger Fourth Amendment protections.[398] Encryption makes accessing the data on the phone difficult, but that difficulty itself does not provide a phone holder with additional Fourth Amendment rights. Once the government has a warrant to search the digital information in a smartphone, as required by *Riley*, it may do so without running afoul of any constitutional violations because the Fourth Amendment "does not protect the individual if the government decides to devote its resources to [successfully] decrypting" the device.[399] Even so, the Court's concerns in *Carpenter* suggest its willingness to revisit the issue in the future if it becomes apparent that the balance between privacy and police power becomes unsettled.

Professor Paul Ohm notes that the Court is dealing with tech exceptionalism, an idea that the exceptionalism of modern

397. Candace Gliksberg, Note, *Decrypting the Fourth Amendment*, 50 LOY. L.A. L. REV. 765, 790 (2017); Manpearl, *supra* note 20, at 191.

398. *See* Orin S. Kerr, *The Fourth Amendment in Cyberspace*, 33 CONN. L. REV. 503, 504 (2001) [hereinafter Kerr II]; Kerr, *supra* note 68.

399. Kerr II, *supra* note 398, at 517.

technology does not sit squarely with previous judicial opinions and conceptions of law.[400] Rather than stick with traditional analogies, the Court in both *Riley* and *Carpenter* looked at the reality of what cell phones produce and, in each opinion, Chief Justice Roberts advised taking into account the sophisticated technologies present today or potentially available in the future,[401] and echoed Justice Brandeis's concern from a case fifty years prior.[402] The modern smartphone is the "perfect surveillance device."[403]

For now, a defendant contesting lawful hacking could argue that the hacking was unreasonable in its scope and manner of execution. To be reasonable in scope and manner of execution, a judge must abide by the particularity requirement for issuing a warrant,[404] and should only permit the collection of information if the collection achieves the stated objectives and is completed in the least intrusive manner possible. A higher standard must apply whenever a judge considers an application for a warrant to access information in a smartphone, and any affidavit supplied in support of an application for a warrant must provide a substantial basis for probable cause.[405] This could mean that those going through the phone must take care to not complete a full scan of the phone and instead only look through the relevant applications in the phone, or that the warrant only permits some types of evidence for collection. For example, those going through a phone to find evidence of child pornography need only to go through the photos and videos to see whether the individual violates any child pornography laws. In *United States v. Zappe*,[406] a magistrate judge issued a warrant to search the defendant's

400. Ohm II, *supra* note 381, at 399.

401. *Id.* at 409.

402. Olmstead v. United States, 277 U.S. 438, 473 (1928) (Brandeis, J. dissenting) ("Subtler and more far-reaching means of invading privacy have become available to the Government. Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.").

403. Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018) ("perfect surveillance device" language).

404. *See generally* Marron v. United States, 275 U.S. 192 (1927).

405. *See, e.g.*, United States v. Calk, 2020 U.S. Dist. LEXIS 116013 (finding that the thirty-seven-page affidavit sufficiently alleged probable cause in a warrant application).

406. United States v. Zappe, No. 5-20-CR-00284-OLG, 2020 U.S. Dist. LEXIS 191122 (W.D. Tex. Oct. 15, 2020).

iPhone for child pornography. The defendant contested the warrant, claiming that it was overbroad in scope. The court rejected the defendant's contentions and explained in detail that the warrant was valid and not overbroad given that "there was ample probable cause to suspect Zappe possessed child pornography" and that iPhones are capable of storing sexually explicit images of young children.[407]

Technology has advanced such that it collects every shard and piece of an individual's life, and when put together, paints a mosaic of users that is more probative than any actual utterance.[408] The latest iPhones do not just store information, like photos and communications. They also track movements and collect other data in service of each user. The Health App, for example, automatically counts each person's steps. Smartphones reveal more information than the search of a house ever could, and even non-content information, or metadata, can be significant in finding someone guilty of a crime. Until digital search technology is developed so that it performs targeted searches on phones, law enforcement agencies must be careful in the data they recover. A judge, when assessing a warrant application, should be aware of these considerations and assess on a case-by-case basis whether the sought-after information would justify the pervasive violation of privacy incurred by the device holder.

V. LAWFUL HACKING AS THE APPROPRIATE SOLUTION TO THE ENCRYPTION DEBATE

To law enforcement, encryption is an impediment to its ability to investigate crimes and hold perpetrators responsible. To users of devices, encryption is a promise of privacy and security. To Apple, encryption is not only a business strategy but an almost guaranteed way to avoid future litigation for failing to guard customer data. In resolving the Encryption Debate, the United States must carefully balance the legitimate interests of law enforcement against the serious security and privacy implications

407. *Id.* at 16.

408. *See* United States v. Jones, 565 U.S. 400, 415-16 (2012) (Sotomayor, J., concurring) (explaining the extent of the government's ability to aggregate data via monitoring).

posed by accessing smartphone data. The central argument for imposing backdoor requirements is efficiency and expediency. Law enforcement agencies want extraordinary access because it allows for quicker results with minimal costs. But until there is a feasible technological solution, lawful hacking is the only viable choice in moving forward in the Encryption Debate. Given the ever-present tension between government surveillance and individual security and privacy, lawful hacking forces each side to compromise while still maintaining its overall goals. Of the two options discussed in this Note, lawful hacking presents itself as the more desirable solution. This Part will proceed by first discussing current legislation proposed in the United States, and then offering normative arguments against the adoption of backdoors, and normative arguments for continued use of lawful hacking.

A. Current US Legislation

In the United States, as concluded by Judge Orenstein,[409] it is up to the legislature whether it wants to provide the government with additional powers, not the judiciary. The Supreme Court has likewise echoed this sentiment in the context of evolving technologies. Justice Samuel Alito opined, "In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[410] The existence of CALEA and the overall legislative scheme suggests that Congress has considered this tension before and that a law requiring a backdoor into an encrypted device is not outside the realm of possibility.[411]

The US Congress is currently grappling with both issues posed by this conundrum and is considering drafted legislation on exactly these issues. On March 5, 2020, US Senator Lindsey Graham introduced in the Senate the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020

409. *See Brooklyn Action*, 149 F. Supp. 3d 341, 376 (E.D.N.Y. 2016).

410. United States v. Jones, 565 U.S. 400, 429-30 (2012) (Alito, J., concurring).

411. If this were the case, Apple and other technology companies might then file a case arguing a violation of their First Amendment rights. This discussion, though relevant, is outside the scope of this Note.

("EARN IT Act").[412] The bill responds to the problem of encrypted technologies perpetuating the sexual exploitation of children[413] by proposing that Section 230 of the Communications Act ("Section 230") be amended to impose liability on internet service providers that provide end-to-end encryption but do not provide law enforcement officials the means to decrypt the material.[414] Section 230 immunizes online platforms from liability for the actions of its users, but the EARN IT Act would remove those protections if those platforms host sexually explicit material depicting children.[415] The EARN IT Act has undergone several revisions in the Senate and is currently accompanied by a House of Representatives version of the bill with similar language.[416]

More directly on point is a subsequent bill introduced by Senator Graham. On June 23, 2020, Senator Graham with Senators Tom Cotton and Marsha Blackburn introduced the Lawful Access to Encrypted Data Act ("LAED").[417] LAED addresses the frustrations expressed by law enforcement agencies tasked with the prevention and detection of matters of national security by effectively requiring technology companies to build in backdoors to their devices.[418] The bill proposes several

412. Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020, S. 3398, 116th Cong. (2020).

413. Keller & Dance, *supra* note 111. *See also* Susan Landau, *A Thoughtful Response to Going Dark and the Child Pornography Issue*, LAWFARE (Nov. 5, 2019), https://www.lawfareblog.com/thoughtful-response-going-dark-and-child-pornography-issue [https://perma.cc/RZZ6-27ML].

414. The bill has gone through several revisions in the Senate, and is accompanied by H.R. 8454. *See* Riana Pfefferkorn, *House Introduces EARN IT Act Companion Bill, Somehow Manages To Make It Even Worse*, CTR. INTERNET & SOC'Y. (Oct. 5, 2020), http://cyberlaw.stanford.edu/blog/2020/10/house-introduces-earn-it-act-companion-bill-somehow-manages-make-it-even-worse [https://perma.cc/W98R-FUEA].

415. Riana Pfefferkorn, *The Senate's twin threats to online speech and security*, BROOKINGS (July 13, 2020), https://www.brookings.edu/techstream/the-senates-twin-threats-to-online-speech-and-security/ [https://perma.cc/D8WF-XNUG].

416. *Id. See also* Pfefferkorn, *House Introduces EARN IT*, *supra* note 414.

417. Lawful Access to Encrypted Data Act, S. 4051, 116th Cong. (2020).

418. Press Release, Senate Judiciary Comm., Graham, Cotton, Blackburn Introduce Balanced Solution to Bolster National Security, End Use of Warrant-Proof Encryption that Shields Criminal Activity (June 23, 2020), https://www.judiciary.senate.gov/press/rep/releases/graham-cotton-blackburn-introduce-balanced-solution-to-bolster-national-security-end-use-of-warrant-proof-encryption-that-shields-criminal-activity [https://perma.cc/82ED-KZD4]; Riana Pfefferkorn, *There's now an even worse Anti-Encryption Bill than Earn It. That Doesn't Make the Earn It Bill OK*, CTR. INTERNET SOC'Y (June 24, 2020), http://cyberlaw.stanford.edu/blog/2020/06/there%E2%80%99s-now-even-worse-anti-

amendments to a variety of current laws, and essentially is an overhaul of the current scheme such that it imposes obligations on almost any provider of encryption services or products.[419] One of the provisions, the "assistance capability directive," even mirrors the TCN language present in both the UK's Investigatory Powers Act and Australia's Assistance and Access Act.[420] The bill has not yet progressed beyond its introduction in the Senate.[421]

The jurisdictions discussed in Part III employ a wide variety of approaches in their own struggles with how to resolve the Encryption Debate. The United Kingdom's IPA,[422] for example, can be read to allow for compulsion of a backdoor. On the other hand, Australia's AAB[423] and Germany's legal scheme[424] articulate a legislative choice not to permit backdoors considering the cybersecurity and privacy concerns. If the United States does choose to pass a bill, the fact that Apple already complies with Chinese localization laws[425] demonstrates that Apple will likely comply with similar laws in each country in which it operates. Still, there are several compelling reasons why the US government should act with caution in passing a law requiring technology companies to modify code permitting extraordinary access.

B. The Normative Argument Against Backdoors

One of the main arguments against backdoors is that they undermine data protection measures.[426] In the last couple of years, several companies have been scrutinized by both the public and by the government for failing to protect customer data. In 2014, Apple came under fire when several celebrities' iCloud

encryption-bill-earn-it-doesn%E2%80%99t-make-earn-it-bill-ok [https://perma.cc/U643-YJLN].

419. Lawful Access to Encrypted Data Act § 3119(a)(1) defines "consumer electronic device" as a device that may be purchased by a member of the general public and one that contains more than 1 gigabyte of storage. That is effectively most electronic devices out there. *See also* Pfefferkorn, *The Senate's twin threats*, *supra* note 415.

420. *See* Pfefferkorn, *The Senate's Twin Threats, supra* note 415.

421. Lawful Access to Encrypted Data Act, S. 4051, 116th Cong. (2020).

422. Investigatory Powers Act 2016, c. 25 (UK).

423. *The Assistance and Access Act 2018* (Austl.).

424. *See* discussion *supra* Section III.c.

425. *See* discussion *supra* Section III.d.

426. *See* Manpearl II, *supra* note 75, at 80.

accounts were hacked.[427] Though the investigation determined Apple's software was not to blame, the fallout from the incident highlighted first, Apple's role as the entity purportedly safeguarding personal information, and second, the vulnerabilities of an insecure system.[428] By compelling Apple to create a backdoor, governments risk exacerbating an already delicate problem. Smartphones have become a critical part of most peoples' lives. Not only do iPhones provide a way for people to communicate, they also serve as storage devices for photos, notes, mementos, and thoughts.[429] iPhones are capable of retaining sensitive information such as passwords to banking applications and other services.[430] US companies lose over US$360 billion per year to intellectual property theft, cybercrime, and costs of downtime.[431] An extensive amount of information would be at risk of being publicly disclosed by malicious third parties who could manipulate the backdoor access code.[432] Additionally, cybersecurity threats from foreign nations alone provides a compelling argument to not adopt measures that weaken any available information security systems. The US government recognized that foreign countries can manipulate existing technologies when Russian forces influenced voters in the 2016 election, when a North Korean group hacked into Sony, and when the popular Chinese app TikTok collected data of US citizens.[433] Government proponents argue that this is simply an easily resolved engineering problem.[434] Mandating a backdoor requirement would exacerbate existing cybersecurity issues. Setting aside the cybersecurity issues, several other issues persist.

Second, in a related fashion, mandating backdoors harms all users of iPhones, not just persons who are individually targeted,

427. Erin Durkin, *Hacker sentenced to prison for role in Jennifer Lawrence nude photo theft*, GUARDIAN (Aug. 29, 2018), https://www.theguardian.com/technology/2018/aug/29/nude-photo-hacker-prison-sentence-jennifer-lawrence-victims [https://perma.cc/JUE5-SS6M].

428. *Id.*

429. *See* Traylor, *supra* note 27, at 490.

430. *See* Manpearl, *supra* note 20, at 169.

431. *See id.*

432. Morrison, *supra* note 72, at 425 (discussing the keys under doormats problem).

433. *Significant Cyber Incidents*, CTR. FOR STRATEGIC & INT'L STUD., https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents [https://perma.cc/GL6U-ZX8J] (last visited Jan. 24, 2021).

434. *See* Barr, *supra* note 115.

and poses a serious risk to minority defendants.[435] If a government compels Apple to modify its code to provide a backdoor into a phone, Apple would have to implement this change on every iPhone for the backdoor requirement to be effective. In its letter to consumers in the *California action*, Apple noted:

> The government suggests this tool could only be used once, on one phone. But that's simply not true. Once created, the technique could be used over and over again, on any number of devices. In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks — from restaurants and banks to stores and homes. No reasonable person would find that acceptable.[436]

There is no way to guarantee that code will not then be used on other phones or not be used in an arbitrary manner. Governments desire the backdoor requirement so it can gain access to phones of suspects, but backdoors affect every phone user. A smartphone is the "perfect surveillance device"[437] and a repository of evidence of potentially guilty actions.[438] Even if the code was written such that third parties cannot manipulate and access the data, there is no guarantee the government itself will not abuse that privilege. The Snowden disclosures demonstrated that the US government used iPhones and other smartphones to spy on both citizens of foreign nations and its own citizens alike.[439] At a local level, if given the tool, police forces may use it in an uneven manner. Disguised racism and unconscious bias may lead to law enforcement using backdoors to investigate persons of specific races and from low-income communities. New York City's Police Department, for example, was found liable for its stop-and-frisk policy, which drew criticism for the disproportionate number of members from the Black and Latinx communities

435. David Ruiz, *There is No Middle Ground on Encryption*, ELEC. FRONTIER FOUND. (May 2, 2018), https://www.eff.org/deeplinks/2018/05/there-no-middle-ground-encryption [https://perma.cc/JD7D-KC2P] ("No system is perfect, but a backdoor system for billions of phones magnifies the consequences of a flaw, and the best and the brightest in computer security don't know how to make a system bug-free.").

436. Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), https://www.apple.com/customer-letter/ [https://perma.cc/2G8F-27J9]; *see also* Traylor, *supra* note 153, at 497.

437. Carpenter v. United States, 138 S.Ct. 2206, 2218 (2018).

438. *See, e.g.*, Riley v. California, 573 US 373, 388 (2014) (critiquing the government's argument on the potential for evidence destruction).

439. *See* discussion *supra* Part I.

being stopped.[440] A ProPublica exposé revealed that artificial intelligence programs used to predict the likelihood of recidivism in sentencing proceedings marked Black defendants as more likely to commit another crime as compared to their White counterparts.[441] Backdoors risk increasing the disparity in the criminal justice system. Since the Snowden disclosures, Apple enhanced its software and increased its encryption measures to prevent this behavior in the future.[442] By providing backdoor access, the potential for government abuse returns.

Third, those committing wrongdoings are less likely to use devices if they know the government can easily gain access to the device.[443] Encrypted phones have *ex-post* value: law enforcement seeks to unlock phones because of the probative evidence that is already on them, not what may be available in the future.[444] However, it is reasonable to assume that once criminals are aware of the vulnerabilities of their devices, they are less likely to use it to record their wrongdoing. As noted by the Electronic Fronter Foundation, an organization that defends civil liberties in the digital world, "it's difficult to believe that many criminals" would not be smart enough to seek alternative methods for securing

440. *See* Floyd v. City of New York, 959 F. Supp. 2d 540 (S.D.N.Y. 2013); *see also Annual Stop-and-Frisk Numbers,* NYCLU, https://www.nyclu.org/en/stop-and-frisk-data [https://perma.cc/TTU4-WP8T] (last visited Jan. 24, 2021).

441. Julia Angwin et al., *Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [https://perma.cc/EV4V-KYDA].

442. *See* Shackelford et al., *supra* note 10; Wakabayashi, *supra* note 8; Sanger & Chen, *supra* note 10.

443. Andrew Crocker, *Deep Dive into Crypto "Exceptional Access" Mandates: Effective or Constitutional—Pick One*, ELEC. FRONTIER FOUND. (Aug. 13, 2015), https://www.eff.org/deeplinks/2015/08/deep-dive-crypto-exceptional-access-mandates-effective-or-constitutional-pick-one [https://perma.cc/ZV4T-96EK] ("In order to believe that [exceptional access] will work, we have to believe there is a set of criminals . . . not smart enough to do *any* of the following: Install an alternative storage or messaging app; Download an app from a website instead of an official app store. Use a web-based app instead of a native mobile app.").

444. *See* Vance 2015, *supra* note 76, at 9 (highlighting some cases where evidence recovered from smartphones was helpful in resolving the matter); *Brooklyn action*, 149 F. Supp. 3d 341, 348 (2016). In the Brooklyn case, Judge Orenstein observed that the FBI first wanted access to the phone to get at evidence inculpating the criminal wrongdoer, but later offered that that the evidence was needed to determine whether there was a drug conspiracy.

their information and communications.[445] A backdoor requirement would not prevent criminals from seeking devices that have encryption technologies or even developing their own, as Al-Qaeda purportedly did.[446]

Last, the type of crimes that law enforcement generally seeks to stop are those which rely on communication between people, so perhaps the conversation should instead shift to end-to-end encryption instead of device encryption.[447] When trying to access phones recovered from terrorists, law enforcement seeks information on other perpetrators and information about future attacks. British officials, for example, sought a terrorist's WhatsApp communications after the terrorist drove a car into pedestrians in central London in an effort to identify others who may be planning more attacks.[448] Local police forces may want evidence about past drug deals or information about future drug deals. The government could work with technology companies to confront end-to-end encryption instead of device encryption. This, however, would be an imperfect solution, but a solution nonetheless. Several types of crimes are not dependent on communications. Often, iPhones can hold probative evidence such as photo and video documentation of a crime. As Manhattan District Attorney Cyrus Vance noted, "That evidence can, among other things, implicate a particular person in a crime, exonerate a person of criminal responsibility, or identify additional victims of a criminal scheme."[449] The sexual exploitation of children serves as the prevalent example of when getting access to the content on an encrypted device is necessary. In the United States, *possession* of any visual depiction of sexually explicit conduct involving a minor violates federal law.[450] Suspected persons possessing the depictions on the device might never transmit the illicit materials, thus evading Apple's software update that scans

445. *See* Crocker, *supra* note 443.

446. *See* Pfefferkorn, *Even Worse Encryption Bill*, *supra* note 418.

447. *See* discussion *supra* Section II.A.

448. *See* discussion *supra* Section II.B.

449. CYRUS VANCE JR., REPORT OF THE MANHATTAN DISTRICT ATTORNEY'S OFFICE ON: SMARTPHONE ENCRYPTION AND PUBLIC SAFETY 3 (Nov. 2018) [hereinafter VANCE 2018].

450. *See* 18 U.S.C. § 2251.

for such images sent in transmission.[451] Without some form of access to the suspected person's iPhone, investigators are unable to gather the very evidence needed to charge him of a federal crime.

C. The Normative Argument for Lawful Hacking

Lawful hacking is an imperfect solution, but it works. Given the considerations articulated above, if law enforcement agencies seek data from an encrypted smartphone, they must be limited to accessing that data through lawful hacking only. The prevention, detection, and resolution of crimes is undoubtedly an important and compelling state interest. To that end, lawful hacking achieves the objective of gathering evidence from a perpetrator without compromising the security and privacy of every iPhone user. There are two main rationales for adopting a law that supports lawful hacking over one that requires backdoors.

First, the very nature of lawful hacking means that law enforcement is more likely to concentrate its resources on the targeted phone.[452] It forces law enforcement to pick and choose the phones they want to expend their resources on. This minimizes the risk of harm to all iPhone users, compared to backdoors where the harm is present for everyone. Arguably, given the concerns of bias in law enforcement, the possibility always remains that law enforcement will pick the phones belonging to minority populations, which can further exacerbate any race disparity issues. But this is less likely to be the case than with backdoors given that law enforcement may instead select phones that have the greatest potential to reveal significant information.

Second, exploiting existing vulnerabilities motivates Apple and other technology companies to build more secure systems. Although this creates the technological arms race that law enforcement is loath to engage in, lawful hacking on its own serves as a check on technology companies' promise of privacy

451. Thomas Brewster, *How Apple 'Intercepts' and Reads Emails When it Finds Child Abuse*, FORBES (Feb. 11, 2020), https://www.forbes.com/sites/thomasbrewster/2020/02/11/how-apple-intercepts-and-reads-emails-when-it-finds-child-abuse/?sh=66b41b5b31c2 [https://perma.cc/4Y2W-RC86].

452. Jacobsen, *supra* note 7, at 585.

and security to its users. The fact that users pay for privacy is indicative of the need to maintain it.[453] Even if Apple users do not take advantage of it, the protection is necessary for those who want it and use the phone in reliance on that promise.

Critics speculate that the technological arms race will only create a new market for lawful hacking. Some fear that lawful hacking can be a bad thing because technology companies can bury trapdoors in their software and sell them later to the highest bidder, demonstrating an abuse of their power for capitalistic gains.[454] Others are concerned that third party companies will exploit the fact their services are valuable to governments and will charge exorbitantly high price tags given that taxpayer money could be put to better use elsewhere.[455] More, this creates a price point that smaller governments with less resources than federal level agencies like the FBI are unable to afford.[456] Even so, to reiterate, by allowing for lawful hacking as the solution to the Encryption Debate, it forces governments to be selective in the phones they want to access without worsening a user's state of security and privacy.

VI. CONCLUSION

Governments seek a simple, efficient, and cost-effective solution, and those discussed have implemented a variety of approaches. The United Kingdom prioritized law enforcement needs and included provisions imposing strict requirements on technology companies in its approach, despite heavy public opinion against its adoption. China took this a step further by ensuring that its legal scheme consistently favors government

453. *But see* Manpearl, *supra* note 20, at 192.

454. *See* Steven Levy, *Cracking the Crypto War*, WIRED MAG. (Apr. 25, 2010), https://www.wired.com/story/crypto-war-clear-encryption/ [https://perma.cc/3RUY-5XVS]; *see also* Dunlap, *supra* note 13, at 1699.

455. *See* Eric Lichtblau and Katie Benner, *F.B.I. Director Suggests Bill for an iPhone Hacking Topped $1.3 Million*, N.Y. TIMES, Apr. 22, 2016, at B3, https://www.nytimes.com/2016/04/22/us/politics/fbi-director-suggests-bill-for-iphone-hacking-was-1-3-million.html [https://perma.cc/VVU4-2T9M]; *see also* Jacobsen, *supra* note 7, at 586.

456. VANCE 2018, *supra* note 449, at 4-5 ("Of course, most state and local law enforcement agencies do not have the resources of the federal government or this office, and cannot afford to rely on expensive lawful hacking solutions in everyday investigations (and, of course, the overwhelming majority of criminal cases in this country are handled by state and local agencies)").

access to private data. At the other end of the spectrum, Germany strives to put individual privacy and security first, even while authorizing the use of lawful hacking. Australia, at present, offers the most balanced approach, though its law remains untested. The United States has yet to decide its stance on the Encryption Debate, and if it does, decisionmakers must balance pressing law enforcement needs with important concerns for privacy and security.

Moving forward, how the United States approaches the Encryption Debate matters. The United States is a major player in the global community,[457] and it is likely that its domestic policies will have an international impact. More, with US technology companies like Apple as some of the largest companies in the world,[458] domestic legislation could alter the nature of the products on the international market.[459] In theory, in response to divergent laws, technology companies can tailor their products to the different demands for each country. For example, Apple can continue to provide secure devices in the Australian market while selling devices with backdoor access in the Chinese market.[460] Whether this is feasible, or even desirable, is unknown.

More, in the modern global state, countries look to each other to develop standards and evaluate options for troubling issues. Australia, for example, used language similar to the UK law, and in turn influenced US pending legislation. A more troubling problem, though, comes up when repressive regimes cite rhetoric from democratic nations to justify its perpetuation of human rights abuses.[461] China, in particular, uses surveillance

457. *See* Bellovin, *supra* note 15, at 5.

458. *See* Manpearl, *supra* note 20, at 167.

459. *See* Manpearl, *supra* note 20, at 166; *see also* James Lewis et al., *The Effect of Encryption on Lawful Access to Communication and Data*, CTR. FOR STRATEGIC & INT'L STUD. 8 (Feb. 2017), https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/encryption/csis_study_en.pdf [https://perma.cc/S2CR-L9Y9].

460. *See* Segal, *supra* note 257, at 8.

461. Bunnie Huang & Edward Snowden, *Against the Law: Countering Lawful Abuses of Digital Surveillance,* J. OPEN ENG'G (July 21, 2016), https://www.tjoe.org/pub/direct-radio-introspection/release/2 [https://perma.cc/6X6G-EA2U]; Matt Burgess, *What is the IP Act and how will it affect you?*, WIRED MAG. (May 8, 2017), https://www.wired.co.uk/article/ip-bill-law-details-passed [https://perma.cc/A7S7-8QFG] ("Its impact will be felt beyond the UK as other countries, including authoritarian regimes with poor human rights records, will use this law to justify their own intrusive

technology to subject its minority Muslim Uyghur population to harsh conditions, and has placed over a million members of the group into concentration camps.[462] It defended an early draft of one of its encryption bills by pointing to the debates in the United States and the United Kingdom, where it seemed evident that Western governments made it a practice to compel technology companies to assist with gathering information from encrypted phones.[463] It was only after condemnation from the international community that China disposed of the problematic provision, but it can revisit that argument when democratic nations pass laws that have the effect of weakening civil liberties. Repressive regimes can justify their egregious actions by pointing to what is considered permissible elsewhere.

Setting aside how individual countries use that information, countries share information gathered from different surveillance techniques with each other, as is evident with the FVEY network. This is even more apparent when the shared information is relevant to several countries, as can be the case with information regarding terrorist groups. More, instead of taking a state-by-state approach, countries could aspire to set international standards and adopt an international approach to the regulation of encryption technologies.[464] These, of course, give rise to concerns of the global surveillance state and whether countries should do that because of what was learned from the Snowden disclosures.

Given this context, this Note sought to provide a thorough explanation of the legal issues and normative concerns driving the global Encryption Debate. As mentioned in the introduction, the Encryption Debate is largely an engineering problem that requires cooperation between technology companies and governments. But, in identifying a path forward, relevant parties must not just consider the implications in one country, but the effect their choice could have globally.

---

surveillance regimes. "Theresa May has finally got her snoopers' charter and democracy in the UK is the worse for it.").

462. Isobel Cockerell, *Inside China's Massive Surveillance*, WIRED MAG. (May 9, 2019), https://www.wired.com/story/inside-chinas-massive-surveillance-operation/; Chris Buckley et al., *How China Turned a City into a Prison*, N.Y. TIMES (Apr. 4, 2019), https://www.nytimes.com/interactive/2019/04/04/world/asia/xinjiang-china-surveillance-prison.html [https://perma.cc/BAB8-C6Y3].

463. *See* Segal, *supra* note 257, at 1.

464. *Id.* at 10.