CRACKS IN THE ARMOR:
LEGAL APPROACHES TO ENCRYPTION

Olivia Gonzalez†

Abstract

Encryption protects digital information from unauthorized access by making it illegible to anyone without an encryption key. While this ensures the security of digital communications, it also prevents the government from accessing evidence it needs for national security investigations. This creates an apparent conflict between the private sector's desire for strong encryption and the government's interest in "back door" access, thus raising the normative question of whether governments should be able to legally require companies to maintain *"back doors" to encrypted information. In view of the significant* impact of this debate on economic, privacy, security, and diplomatic interests of states around the world, this Article explores two lines of inquiry: First, what legal frameworks should courts and legislators use to approach encryption? Second, which framework produces the best policy outcomes—in particular, which stakeholders are benefitted or harmed under each approach? To answer these questions, this Article examines legal approaches to encryption in the U.S. and U.K., countries with contrasting policies on the subject. It evaluates the pros and cons of each approach, situating encryption within existing legal *frameworks. This includes the First Amendment argument of "code as free speech," government investigatory powers under the Fourth Amendment, and the U.K.'s Investigatory Powers Act permitting government-*mandated back doors. This is the first paper clarifying, surveying, and comparing the legal approaches to encryption in the U.S. and U.K. Such a comparative analysis explaining the consequences of each legal approach could help countries choose the most effective approach to encryption. By applying existing laws to the novel problems posed by encryption, this Article generates new evidence against the implementation of encryption back doors.

† Olivia Gonzalez is an attorney at the New York Office of Brown Rudnick LLP. Msc., Oxford University (2017); J.D., Fordham University School of Law (2016); B.A., New York University (2013). The views represented here are solely those of the author. She is grateful to Dr. Anne-Marie Oostveen of the Oxford Internet Institute and Dr. Rebecca Williams of the Oxford Law Faculty for their advice and mentorship in the production of this Article. She is also indebted to a number of others for formative conversations in the early stages of this work. In particular, discussions with Ariel Ezrachi, Ashley Deeks, Viktor Mayer-Schönberger, Ralph Schroeder, Greg Taylor, Joss Wright, and Paul Yowell were essential in the development of the ideas expressed here. The author is also grateful to Eric Freiman and Nate Chumley for their research assistance.

TABLE OF CONTENTS

I. INTRODUCTION

The question of whether a government can legally mandate access to encrypted data was revitalized in 2016 by the dispute between Apple and the U.S. Federal Bureau of Investigation (FBI).[1] In that dispute, the FBI sought access to the encrypted iPhone of a terrorist shooter in San Bernardino, California.[2] The iPhone 5c was protected by encryption-based security measures, making it impossible to access the contents without changing the software.[3] For simplicity, this kind of access is often referred to as a "back door" to the encrypted communications. When the FBI sought a court order requiring Apple to build one, their refusal re-ignited an old debate about government investigatory power, privacy, and global internet governance.

[1] *In re* An Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. ED 15-0451M, 2016 U.S. Dist. LEXIS 20543 (C.D. Cal. Feb. 16, 2016).

[2] Government's *Ex Parte* Application for Orders Compelling Apple, Inc. to Assist Agents in Search; Memorandum of Points of Authorities at 3 [hereinafter *Ex Parte* Application], https://www.justice.gov/usao-cdca/page/file/1066141/download; *In re the Search of An Apple iPhone*, 2016 U.S. Dist. LEXIS 20543, at *1.

[3] *Ex Parte* Application, *supra* note 2, at 6.

The central problem at the heart of the encryption debate is that back doors fundamentally undermine the security of networks.[4] If a message is intercepted by the government or telecommunications operator, it remains gibberish unless the interceptor has a decryption key.[5] End-to-end encryption, by definition, means that only the sender and receiver have access to a key that can decrypt an electronic communication.[6] Moreover, modern encryption is difficult to break by guessing keys because the "number of possible keys vastly exceeds the number of guesses that even today's fastest computers can make in a reasonable time frame."[7] "Strong" encryption, or encryption devoid of back doors, means that the government has no direct access to encrypted communications in cases of national security.[8] However, introducing such a back door means creating a security vulnerability that can be exploited by malicious actors.[9]

In this manner, the creation of back doors or other types of "exceptional access" would compromise network security as well as individual privacy.[10] The tension between these competing values led to the politicization of the encryption debate. Tim Cook, Apple's CEO, argued that the government's request for a back door "would undermine the very freedoms and liberty our government is meant to protect."[11] The FBI's brief before the court argued that Apple's refusal "would frustrate the execution of a valid warrant and thwart the public interest in a full and complete investigation of a horrific act of terrorism."[12] The apparent conflict between these approaches and the importance of sensible encryption policy are the primary motivators of this Article.

While the use of encryption dates back to ancient Greece, its modern applications pose important new problems. Encryption governance has high-stakes repercussions in the realms of economics, security, diplomatic relations, and privacy.[13] Economically, the presence of legally mandated back doors could deter businesses from operating in certain countries, redirecting investment to

[4] Harold Abelson et al., *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, 1 J. CYBERSECURITY 69, 70 (2015).

[5] John Villasenor, *No, the Laws of Australia Don't Override the Laws of Mathematics*, BROOKINGS INST. (July 17, 2017), https://www.brookings.edu/blog/techtank/2017/07/17/no-the-laws-of-australia-dont-override-the-laws-of-mathematics.

[6] *Id.*

[7] *Id.*

[8] As this Article will later explain, there may be indirect ways for law enforcement to access the encrypted communications.

[9] *See generally* IDAHO NAT. LAB., CYBER THREAT AND VULNERABILITY ANALYSIS OF THE U.S. ELECTRIC SECTOR 14 (2017) (discussing back door remote access).

[10] *Id.*

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

[12] Government's Motion to Compel Apple to Comply with this Court's Feb. 16, 2016 Order Compelling Assistance in Search at 6–7, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, ED No. CM 16-10 (C.D. Cal. Feb. 19, 2016).

[13] *See* Kaveh Waddell and National Journal, *How Much is Encryption Worth to the Economy?*, THE ATLANTIC (Nov. 9, 2015), https://www.theatlantic.com/politics/archive/2015/11/how-much-is-encryption-worth-to-the-economy/458466 ("The tech industry, however, argues that consumers want better security and privacy and that a weaker encryption standard would be a huge economic hit to U.S. companies, because consumers would shift to apps and services with strong encryption made overseas.").

countries that allow strong encryption.[14] If businesses perceive a higher risk of data breach, privacy litigation, or a prohibitive cost of compliance, they may refrain from operating in countries with back door requirements.[15] Since 2007, the cybersecurity market has grown more than thirty times and is now valued at $120 billion.[16] This suggests that businesses perceive digital vulnerability to be risky and costly enough to warrant hiring cyber security firms.[17] Additionally, the risk of litigation may be high enough to merit hiring a third party that could be indemnified in case of a lawsuit.[18] In a number of jurisdictions like the U.S., firms can "indemnify" or share litigation costs with a third party that was responsible for the liability.[19] Indemnity is an obligation by a party to compensate for a particular loss suffered by another.[20] From a security standpoint, the U.S. and U.K. governments' primary concern is that a lack of back doors could create a refuge for terrorist communication insulated from law enforcement surveillance.[21] However, the imposition of back doors means that sensitive information is more vulnerable to cyberattacks.[22]

Encryption also has important consequences for international legal and diplomatic relations.[23] Multi-national corporations like Apple receive requests for legal assistance from governments around the world.[24] A private company's use of strong encryption means that it will be unable to comply with a foreign government's request to produce information for a criminal investigation.[25] Until jurisdictional norms of internet governance develop, a multi-national corporation may be exposed to conflicting legal obligations.[26] Moreover, the existing diplomatic network of mutual legal assistance treaties (MLATs)

[14] *Id.*

[15] *Id.*

[16] Julie Charpentrat, *Cyberattacks Prompt Massive Security Spending Surge*, PHYS.ORG (May 18, 2017), https://phys.org/news/2017-05-cyberattacks-prompt-massive-surge.html.

[17] *See id.* (explaining that attacks in digital privacy have created a demand for cyber security firms).

[18] *See* Judith H. Germano, *Third-Party Cyber Risk and Corporate Responsibility*, CTR. FOR CYBERSECURITY (Feb. 2017), https://www.lawandsecurity.org/wp-content/uploads/2017/02/Germano.NYU_.ThirdPartyRiskWhitepaper.Feb2017.pdf ("To address these concerns, companies must define security procedures and policies, and consider liability and indemnification provisions that correspond to the value of data at issue.").

[19] *See* Adeola Adele et al., *More Vendors, More Problems*, WILLIS TOWERS WATSON (Dec. 21, 2016), https://www.willistowerswatson.com/en/insights/2016/12/more-vendors-more-problems (explaining how "[i]n addition to warranties and damages limitations, most vendors contracts will contain some sort of indemnity provision.").

[20] *Id.* (illustrating that one such indemnity clause could require the vendor to "defend and indemnify Customer against any third-party claim . . . .").

[21] *See generally* Robby Mook, *Encryption Keeps Us Safe. It Must Not Be Compromised With 'Backdoors'*, THE GUARDIAN (Feb. 12, 2018), https://www.theguardian.com/commentisfree/2018/feb/12/encryption-safe-hillary-clinton-secure-backdoors-privacy (explaining how "for those companies to simply create a backdoor—a special set of keys that allow law enforcement to 'unlock' encrypted communications of suspected criminals—would be wrong.").

[22] *Id.*

[23] *See generally* ASHLEY DEEKS, HOOVER INST., THE INTERNATIONAL LEGAL DYNAMICS OF ENCRYPTION (Oct. 11, 2016), https://www.hoover.org/sites/default/files/research/docs/deeks_webreadypdf.pdf (discussing importance of encryption software on international relations).

[24] *Id.* at 3–5.

[25] *Id.*

[26] *Id.*

between countries would be disrupted by differences in encryption policy.[27] For example, an international version of the Apple-FBI dispute could arise where the French government seeks to compel backdoor access to encrypted communications. At first glance, Apple would not need to build back doors to comply with French law.[28] On the other hand, its lack of compliance might mean that the U.S. is in breach of a MLAT with France which requires cooperation in law enforcement investigations.[29]

Moreover, the MLAT landscape has recently been altered with the March 2018 passage of the Clarifying Lawful Overseas Use of Data (CLOUD) Act.[30] The CLOUD Act provided a legislative answer to the question of whether a U.S. company could be forced to retrieve digital communications from customers located outside the U.S.[31] Under the CLOUD Act, companies are required to comply with government requests for data even if it is stored on servers outside the U.S.[32] Since requests like these were typically governed by individual MLAT treaties, the CLOUD Act represents a shift in international data sharing with the U.S.[33] The implications of the CLOUD Act for the exchange of encrypted information remain unclear. However, these changes could impact diplomatic relations between countries and alter the international norms of internet governance. Since encryption is a ubiquitous technology used to secure many types of information, the resolution of these legal issues could set an important precedent for future technology cases.

In addition to its importance at the corporate or government level, encryption is a safeguard of individual privacy and civil liberties.[34] End-to-end encryption protects individual data from surveillance and hacking.[35] Trust in the privacy of digital communications also lubricates a free exchange of ideas.[36]

[27] *See* Mutual Legal Assistance, U.S.-U.K., Jan. 6, 1994, 104th Cong., 1st Sess., Treaty Doc. 104-2, Exec. Rpt. 104-23 (discussing the MLAT between the U.S. and the U.K.). *E.g.*, 80 Stat. 271; 1 U.S.C. § 113 (2018) ("Treaty Between the United States of America and the United Kingdom of Great Britain and Northern Ireland").

[28] *See generally* BHAIRAV ACHARYA ET AL., NEW AM., DECIPHERING THE EUROPEAN ENCRYPTION DEBATE: FRANCE (July 31, 2017), https://www.newamerica.org/oti/policy-papers/deciphering-european-encryption-debate-france (discussing France's encryption framework).

[29] *See also* Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme, 145 F. Supp. 2d 1168, 1171 (N.D. Cal. 2001) (discussing the case where the U.S. internet company *Yahoo!* was sued in a French court for allowing its platform to sell Nazi memorabilia, in violation of French law. The French court ultimately ruled in *Yahoo!*'s favor, easing global fears that national laws would increasingly be imposed on international internet companies. This illustrates the principle that the jurisdiction of national courts over internet companies is limited).

[30] *See generally* Niki Edmonds, *CLOUD Act Opens Up User Data to Foreign Governments*, JOLT DIG. (Apr. 1, 2018), https://jolt.law.harvard.edu/digest/cloud-act-opens-up-user-data-to-foreign-governments (explaining what the CLOUD Act is).

[31] *Id.*

[32] *Id.*

[33] *Id.*

[34] *See* Neema Singh Guliana, *The Cloud Act is a Dangerous Piece of Legislation*, ACLU (Mar. 13, 2018), https://www.aclu.org/blog/privacy-technology/internet-privacy/cloud-act-dangerous-piece-legislation (discussing how the Cloud Act is a threat to individual privacy).

[35] However, it is important to note that most types of encryption do not protect metadata or a communicator's identifying factors such as an IP address. *See* David Kaye, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, ¶ 62 U.N. Doc. A/HRC/29/32 (May 22, 2015).

[36] *Id.* at ¶¶ 11–12.

According to UN Special Rapporteur David Kaye, encryption technologies "enable private communications and can shield an opinion from outside scrutiny, particularly important in hostile political, social, religious and legal environments."[37] Encryption thus ensures that speech will remain unburdened by the "chilling effect" of surveillance.[38] The "chilling effect" theory posits that fear of legal penalty suppresses or alters speech.[39] A 2016 study by Jonathon Penney found empirical evidence for the proposition that surveillance "chills" online speech.[40] Avoiding the suppression of speech in this manner has long been a motivation of free speech regulation in the U.S. and, more recently, in the U.K.[41] These considerations serve to further illustrate the importance of a coherent legal framework around encryption.

Through a comparative lens, the U.S. and U.K. represent helpful test cases, as they take opposite legal approaches towards encryption.[42] Given the absence of legislation directly addressing encryption, the U.S. might situate encryption into its existing constitutional structure without creating any new laws.[43] As Part I of this Article will note, one legal approach involves treating code (including encryption code) like speech under U.S. constitutional law.[44] Alternatively, encryption could be analyzed in terms of government investigatory power and search warrants.[45] One aim of this Article is to assess the persuasiveness of these approaches and compare them to the U.K.'s regulatory counterpart. In the U.K., by contrast, encryption falls directly under a legislative scheme subject to a "proportionality" analysis.[46] Under this analysis, a judge or official will evaluate the government action to determine whether it was necessary and proportional to the severity of the public needs.[47] However, determining whether a government action was proportional requires a clear understanding of the normative policy considerations. Since the available

[37] *Id.* at ¶ 22.

[38] Jonathon Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERKELEY TECH. L.J. 118, 137–43 (2016) (showing a statistically significant decline in traffic for "privacy-sensitive" Wikipedia articles after revelations of NSA surveillance in June 2013).

[39] *Id.*

[40] *Id.*

[41] *See* Weiman v. Updegraff, 344 U.S. 183, 195 (1952) (Frankfurter, J., concurring) (using the phrase "chilling effect" for the first time in U.S. First Amendment law); *see* Derbyshire Cty. Council v. Times Newspaper Ltd. [1993] A.C. 534 (recognizing the existence of a chilling effect on legitimate expression); *see also* Walker v. City of Birmingham, 388 U.S. 307, 344–45 (1967) (Brennan, J., dissenting) ("We have molded both substantive rights and procedural remedies in the face of varied conflicting interests to conform to our overriding duty to insulate all individuals from the chilling effect upon exercise of First Amendment freedoms generated by vagueness, overbreadth and unbridled discretion to limit their exercise.").

[42] *See generally World Map of Encryption Laws and Policies*, GLOB. PARTNERS DIG. (last visited Mar. 9, 2019), https://www.gp-digital.org/world-map-of-encryption (showcasing how the laws of the United States and the United Kingdom differ with respect to cybersecurity).

[43] *See generally* DEEKS, *supra* note 23 (discussing national encryption approaches).

[44] For complete discussion, *see infra* Part I.A. for discussion on encryption and U.S. First Amendment jurisprudence.

[45] For complete discussion, *see infra* Part I.B. for discussion on encryption and U.S. Fourth Amendment jurisprudence.

[46] For complete discussion, *see infra* Part II for discussion on encryption and U.S. Fourth Amendment jurisprudence.

[47] *See generally* Cynthia Lee, *Reasonableness with Teeth: The Future of Fourth Amendment Reasonableness Analysis*, 81 MISS. L.J. 1133 (2012) (discussing the proportionality analysis).

policy options are constrained by the law, it is important to ask which stakeholders are harmed and benefited under each legal approach. This Article will involve a twofold inquiry animating the analysis in each chapter. First, it will examine what legal arguments courts and legislators should use to approach encryption. This includes the First Amendment argument of "code as free speech," government investigatory powers under the Fourth Amendment, and the U.K.'s Investigatory Powers Act permitting government-mandated back doors.[48] Based on the existing approaches, this Article will explain which framework produces the best policy outcomes, considering the harms and benefits to relevant stakeholders. This Article comes to a number of conclusions for each area of legal analysis. Among them, it concludes that legal doctrine should regulate different types of code differently; that a warrant should be universally required when the government "lawfully hacks" encrypted devices; and that requiring back doors may not be "necessary and proportionate" as required by U.K. law.[49]

Encryption technologies will only grow in ubiquity, particularly as everyday devices and appliances also become connected to the internet.[50] The rise of these networked devices will increase the importance of the security and privacy encryption provides.[51] Network security, privacy, and law enforcement aims will be realized only if there is an adequate approach to dealing with the problems encryption raises. While the encryption debate appears, at first sight, to be a straightforward case of balancing privacy and security, the equities to be balanced are in fact more complex. Since the U.S. and U.K. have opposing views on encryption regulation, this Article evaluates the relative benefits and consequences of each approach.[52] A comparative analysis between two countries with opposite regulatory schemes yields important insights about the soundness of each encryption policy. Special attention will be paid to the ethical, legal, and policy consequences of encryption back doors.

The analysis proceeds in two parts: Part I focuses on legal approaches to encryption under U.S. law, examining how encryption could be conceptualized under existing U.S. case law. There are multiple areas of U.S. law to which encryption might apply. This Part will focus on two of the most notable legal

[48] *See* Graham Smith, *Investigatory Powers Act: Back Doors, Black Boxes, and Tech Capability Regs*, ARS TECHNICA (May 8, 2017), https://arstechnica.com/tech-policy/2017/05/investigatory-powers-act-legal-analysis (explaining the Act and how it permits backdoors in general).

[49] "Lawful hacking" is a term of art sometimes employed to describe the government's use of existing software vulnerabilities to access information for investigatory purposes. *See generally* Steven M. Bellovin et al., *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 NW. J. TECH. & INTELL. PROP. 1 (2014) (discussing current vulnerabilities in hacking); Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 GEO. L.J. 989, 991–92 (2018) (covering the weaknesses in encryption).

[50] *See generally Cyber Attacks Spawn Fear of Household Appliances*, IRISH TIMES (Oct. 25, 2016), https://www.irishtimes.com/business/technology/cyber-attacks-spawn-fear-of-household-appliances-1.2841762 (discussing generally how common household items such as thermostats and fridges are connected to the Internet).

[51] *See id.* (explaining how cyberattacks have created a fear that household appliances, connected to the network, will be negatively affected).

[52] *See* DEEKS, *supra* note 23 (comparing the U.K. and other foreign states' perspectives on encryption to the U.S. perspective); Andrada Coos, *EU vs US: How Do Their Data Privacy Regulations Square Off?*, ENDPOINT PROTECTOR (Jan. 17, 2018), https://www.endpointprotector.com/blog/eu-vs-us-how-do-their-data-protection-regulations-square-off (discussing privacy regulations in the EU and U.S.).

theories. Part I.A. will discuss the argument that encryption, and all other types of code, should be regulated as "speech." This Part will evaluate the persuasiveness of this argument and its potential impact on encryption policy. Part I.B. will focus on an alternative legal theory suggesting that encryption should be regulated as a type of government "search." This theory involves examining the legality of encryption technologies through the prism of government investigatory power. Rather than arguing for one approach in particular, this Part examines the nuanced strengths and weaknesses of each.

Part II discusses encryption under U.K. law. Unlike the U.S., the U.K. has legislation that directly governs encryption and permits the government to mandate back doors.[53] This eliminates the need for analyzing constitutional theories in order to determine encryption's place in the legal system. Instead, this Part will focus on a statutory analysis of the relevant provisions in the Investigatory Powers Act (IPA). In order for the U.K. government to order a telecommunications operator to install a back door, the Secretary of State would have to determine that the order's requirements are "necessary and proportional."[54] This "proportionality inquiry" is a four-part test that these orders must pass.[55] The purpose is to evaluate government actions for possible overreach. Accordingly, this Part will explain the policy considerations influencing the analysis under each factor. This Part will ultimately argue that mandated encryption back doors might fail certain prongs of this proportionality review. Throughout, this Article will examine how each legal interpretation harms or benefits stakeholders like corporations, government, and civil society.

II. BACKGROUND

Two primary misconceptions underlie the current debate about encryption policy. The first involves a technical misunderstanding of how encryption works. Encrypted communications are often seen as discrete objects that can be individually "unlocked" or "decrypted."[56] Law enforcement agencies sometimes view a technology company employing encryption as stubborn for refusing to "decrypt" a particular encrypted communication in a criminal investigation.[57] But unless the company has retained the encryption key, it is

[53] Regulation of Investigatory Powers Act 2000, c. 23 (Eng.); Joël Valenzuela, *UK Bans End-to-End Encryption, Mandates Government Authority Over Encrypted Technologies*, COINTELEGRAPH (Dec. 2, 2016), https://cointelegraph.com/news/uk-bans-end-to-end-encryption-mandates-government-authority-over-encrypted-technologies.

[54] Asaf Lubin, *The Investigatory Powers Act and International Law: Part I*, UCL J.L. & JURIS. BLOG (2016), https://blogs.ucl.ac.uk/law-journal/2016/12/26/the-investigatory-powers-act-and-international-law-part-i.

[55] *Id.*

[56] *See generally Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety*, MANHATTAN DIST. ATTORNEY'S OFF. (Nov. 2018), http://manhattanda.org/sites/default/files/Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety:%20An%20Update.pdf (discussing the encryption of smartphones with respect to public safety).

[57] Jonathan Haynes, *Back Door Access to WhatsApp? Rudd's Call Suggests A Hazy Call Suggests a Hazy Grasp of Encryption*, THE GUARDIAN (Mar. 27, 2017), https://www.theguardian.com/technology/2017/mar/27/amber-rudd-call-backdoor-access-hazy-grasp-encryption (explaining that an encrypted message cannot be decrypted except by the user who has the private key).

impossible for it to "decrypt" messages protected by end-to-end encryption.[58] Only a user with the private encryption key can decrypt an encrypted communication.[59] A WhatsApp message, for instance, can only be decrypted by the holders of the private key—the sender and recipient.[60] This means that in order to comply with future government requests for encrypted information, the company would need to build its products using a weaker form of encryption that allows for exceptional access.[61] The legal implication is that a government would need to have the authority to compel a private corporation to *build* something for a government purpose, namely, exceptional access. A 2015 paper written by a team of computer scientists entitled *Keys Under Doormats* argues that law enforcement has "failed to account for the risks inherent in exceptional access systems."[62] This lack of appreciation for the economic, security, privacy, and diplomatic consequences of back doors is partially rooted in a technical misunderstanding of encryption.

The second political misconception is that the encryption debate arises out of a clash between the government's interest in security and the private sector's prioritization of privacy. Under this narrative, technology companies encrypt communications in the name of privacy despite weighty national security reasons to maintain back doors. In his article *Beyond Cheneyism and Snowdenism,* Cass Sunstein explains that in the domain of national security, "Cheneyists" favor a "precautionary principle, insisting that it is better to be safe than sorry, and hence a range of important safeguards including widespread surveillance, are amply justified to prevent loss of life."[63] Conversely, "Snowdenists" who object to those initiatives, particularly widespread surveillance, "respond with a Precautionary Principle of their own, seeking safeguards against what they see as unacceptable risks to privacy and liberty."[64] It is this kind of bifurcation that informs the encryption debate and produces ineffective policy measures.

Indeed, the encryption policy debate is more complex than a disagreement about these values.[65] Privacy is a weighty motivating factor for encryption, particularly since technology companies benefit financially from their

[58] *See id.* (explaining that an encrypted message cannot be decrypted except by the user who has the private key).

[59] *Id.*

[60] *Id.*

[61] *See* Bruce Schneier, *The Importance of Strong Encryption to Security*, SCHNEIER ON SEC. (Feb. 25, 2016) [hereinafter Schneier I], https://www.schneier.com/blog/archives/2016/02/the_importance_.html (discussing how allowing back-door access weakens encryption).

[62] *See* Abelson et al., *supra* note 4 (addressing how governmental back-door access weakens encryption security).

[63] Cass Sunstein, *Beyond Cheneyism and Snowdenism*, 83 U. CHI. L. REV. 271, Abstract (2015) [hereinafter Sunstein I] (quoting Dick Cheney: "Sooner or later, there's going to be another attack and they'll have deadlier weapons than ever before . . . .").

[64] *Id.* at 273 (quoting Edward Snowden: "If we can't have the privacy of our bedrooms, if we can't have the privacy of our notes on our computer, if we can't have the privacy of our electronic diaries, we can't have privacy at all.").

[65] Bruce Schneier, *The Value of Encryption*, SCHNEIER ON SEC. (Apr. 2016), https://www.schneier.com/essays/archives/2016/04/the_value_of_encrypt.html [hereinafter Schneier II] ("The FBI paints this as a trade-off between security and privacy. It's not. It's a trade-off between more security and less security.").

reputations as privacy-protectors.[66] However, the security-related motivations for encrypting data are just as weighty as the privacy incentives. The existence of back doors means that they can also be exploited by malicious actors.[67] Unauthorized access to encrypted information by one such malicious actor could enable cyberattacks that result in loss of life or property.[68] Security vulnerabilities or back doors could also be exploited by nation-states to carry out acts of war.[69] Since security can also be cited in support of strong encryption, the debate about encryption policy cannot be reduced to a tug-of-war between privacy and security.[70] The politicization of encryption makes it challenging to design a regulatory strategy. On one hand, depoliticizing the policy questions allows for the possibility of consensus.[71] On the other hand, values like privacy and security appropriately motivate decisions in encryption policy.[72] As Jeremy K. Kessler and David Pozen note in their metatheoretical paper on the life cycle of legal theories, lawyers sometimes "seek to negotiate highly politicized legal conflicts through the introduction of decision-making frameworks that abstract away from the central values in contention."[73] Acknowledging the competing values plays an important role in understanding the encryption debate. However, the precise weight to be given to the different values being balanced involves taking stock of the harms and benefits of each policy choice.

The encryption debate is important because it involves a larger conversation about the interaction between law and technology. It poses questions about how the two should interact, given that law will always trail behind technology. One such question is whether the problems posed by emerging technologies should be treated as *new* issues for the law. This would involve passing a new law for every new problem that arises from an advance in technology. Alternatively, the problems posed could be situated within existing legal systems. The latter approach sometimes produces tortured legal arguments, as the law bends to accommodate modern problems. According to

[66] David Hoffman, *Privacy is a Business Opportunity*, HARV. BUS. REV. (Apr. 18, 2018), https://hbr.org/2014/04/privacy-is-a-business-opportunity; Tripp Mickle, *Apple Exerts Power as Privacy Protector*, WALL ST. J. (Jan. 31, 2019), https://www.wsj.com/articles/apple-exerts-power-as-privacy-protector-11548982840.

[67] Schneier I, *supra* note 61; Amie Stepanovich & Michael Karanicolas, *Why An Encryption Backdoor for Just the "Good Guys" Won't Work*, JUST SEC. (Mar. 2, 2018), [hereinafter Stepanovich & Karanicolas] https://www.justsecurity.org/53316/ criminalize-security-criminals-secure.

[68] *See* Ioannis Agrafiotis et al., *A Taxonomy of Cyber-harms: Defining The Impacts of Cyber-Attacks and Understanding How They Propagate*, 4 J. CYBERSECURITY 1 (2018) (discussing the types of harms caused by cyberattacks); Luke Probasco, *Encryption Requirements for Banks & Financial Services*, TOWNSEND SEC. DATA PRIVACY BLOG (Apr. 25, 2017), https://info.townsendsecurity.com/encryption-requirements-for-banks-financial-services.

[69] Ellen Nakashima, *When Is a Cyberattack an Act of War?*, WASH. POST (Oct. 26, 2012), https://www.washingtonpost.com/opinions/when-is-a-cyberattack-an-act-of-war/2012/10/26; Kate O'Flaherty, *Cyber Warfare: The Threat from Nation States*, FORBES (May 3, 2018, 8:17 AM), https://www.forbes.com/sites/kateoflahertyuk/2018/05/03/cyber-warfare-the-threat-from-nation-states.

[70] Schneier II, *supra* note 65.

[71] *See* Jeremy K. Kessler & David Pozen, *Working Themselves Impure: A Life Cycle Theory of Legal Theories*, 83 U. CHI. L. REV. 1819, 1826 (2016) [hereinafter Kessler & Pozen] (describing the theory of de-politicization to overcome legal conflict).

[72] *See* DEEKS, *supra* note 23 (stating that encryption policy can be motivated by a variety of privacy and security values).

[73] Kessler & Pozen, *supra* note 71, at 1826.

Lawrence Lessig, the principles underlying existing law should be "translated" before being applied to emerging technologies.[74] As such, Lessig is more inclined to situate these new problems within existing law instead of understanding them as unique. However, this approach requires consideration of whether existing laws will suffice in every case.

A related question is whether the dynamic nature of technological development should motivate courts to take a restrained approach to ruling on problems rooted in new technologies. Ruling prematurely on a problem grounded in emerging technologies risks perverting precedent and creating problematic legal rules in the future. This is the view espoused by Cass Sunstein in his 1996 article, *Constitutional Caution*, which warns against judicial activism in the face of fluctuating technologies.[75] Under his view, technology changes too frequently for courts to produce a coherent doctrine applicable to future cases.[76] Then again, active judicial participation in technology lawsuits enables a case-by-case analysis. While parliamentary legislation may apply universally, it may not be equally wise in every case. Courts can issue more specific rulings and may regulate encryption more effectively than one-size-fits-all legislation.[77] Lessig, in a 1996 article, takes a more moderate approach on the question of judicial activism. He notes that "[w]hen judgments are tied to fairly clear historical traditions, when limitations are compellingly similar to original constraints, when a court can affect what plainly appears to be a mere translation . . . here, a court should act to limit."[78] The polyphony of multiple court opinions may ultimately produce better policy than one congressional act. This narrow approach could produce more informed but possibly less consistent doctrine.

Finally, the encryption debate poses important questions about the global governance of the Internet, more generally. From an international perspective, it is complicated to resolve the jurisdictional problems in technology cases since the Internet is necessarily a cross-border phenomenon. Open questions remain about which country, sector, or international organization regulates new technologies. The encryption debate demands consideration about the relationship between law and technology. Issues raised by the encryption debate will play an important role in the development of norms in Internet governance in the future.

[74] Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L.J. 869, 903 (1996).

[75] Cass R. Sunstein, *Constitutional Caution: The Law of Cyberspace*, U. CHI. LEGAL F. 361, 370 (1996) [hereinafter Sunstein II]; *see also* Orin Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 804 (2004) [hereinafter Kerr I] ("The view that the Fourth Amendment should be interpreted broadly in response to technological change has been embraced by leading theorists of law and technology such as Lawrence Lessig, and nearly everyone else who has written on the intersection of technology and criminal procedure.").

[76] Sunstein II, *supra* 75, at 374.

[77] Lessig, *supra* note 74, at 908–09.

[78] *Id.* at 908.

III. PART I: ENCRYPTION UNDER US LAW

A. *First Amendment Arguments: Code as Speech*

While the legal landscape on encryption is still developing, the Apple-FBI litigation tested arguments on the reach of government power in encryption cases.[79] One argument by Apple involves conceptualizing code as a form of speech.[80] Under U.S. law, the government cannot regulate free speech unless it falls into one of approximately nine narrow categories.[81] These categories include pernicious types of speech like defamation, child pornography, and incitement to imminent lawless action.[82] While undoubtedly forms of expression, the First Amendment does not protect them from government regulation because of their destructive nature.[83] Speech outside these narrow categories is highly protected under U.S. law, meaning that the government is constitutionally limited in its regulation of speech.[84] The following subsection will analyze the First Amendment arguments made by Apple in its litigation against the FBI.

1. *Apple's Arguments and the First Amendment Machinery*

In the Apple-FBI case, Apple argued that a court order requiring them to "decrypt" the iPhone information would violate the First Amendment.[85] In particular, Apple argued that the request would amount to "compelled speech and viewpoint discrimination in violation of the First Amendment."[86] The Supreme Court has held that where the government seeks to compel speech, the machinery of First Amendment protections is triggered.[87] This means that the

[79] Arjun Kharpal, *Apple vs FBI: All You Need to Know*, CNBC (Mar. 29, 2016, 6:34 AM), https://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html; Danny Yadron et al., *Inside the FBI's Encryption Battle With Apple*, THE GUARDIAN (Feb. 18, 2016), https://www.theguardian.com/technology/2016/feb/17/inside-the-fbis-encryption-battle-with-apple.

[80] The argument that code should be treated as speech has been made before the Apple-FBI case. For prior academic treatment, see Alex Colangelo & Alana Maurushat, *Exploring the Limits of Computer Code as a Protected Form of Expression: A Suggested Approach to Encryption, Computer Viruses, and Technological Protection Measures*, 51 MCGILL L.J. 47 (2006); Stuart Minor Benjamin, *Algorithms and Speech*, 161 U. PA. L. REV. 1445 (2013); Tim Wu, *Machine Speech*, 161 U. PA. L. REV. 1495 (2013); Adam C. Bonin, *Protecting Protection: First and Fifth Amendment Challenges to Cryptography Regulation*, 1996 U. CHI. LEGAL F. 495 (1996).

[81] *Which Types of Speech Are Not Protected by the First Amendment?*, FREEDOM F. INST. [hereinafter FREEDOM F. INST.], https://www.freedomforuminstitute.org/about/faq/which-types-of-speech-are-not-protected-by-the-first-amendment (last visited Mar. 10, 2019).

[82] *Id.*

[83] *See* Andrew Koppelman, *Revenge Pornography and First Amendment Exceptions*, 65 EMORY L.J. 661 (2016) (stating that a first amendment exception must be sufficiently harmful to overcome protection of speech).

[84] Kathleen Ann Ruane, *Freedom of Speech and The Press: Exceptions to The First Amendment*, CONG. RES. SERV. (Sept. 8, 2014), https://fas.org/sgp/crs/misc/95-815.pdf; *Free Speech: What's at Stake*, ACLU, https://www.aclu.org/issues/free-speech (last visited Mar. 10, 2019).

[85] Apple Inc. Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search and Opposition to Government's Motion to Compel Assistant, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, ED No. CM 16-10 (C.D. Cal. Feb. 19, 2016).

[86] *Id.*

[87] Riley v. Nat'l Fed'n of Blind, 487 U.S. 781, 796–99 (1988).

government could only compel speech subject to an "exacting scrutiny" where the government action is narrowly tailored to obtain a compelling state interest.[88] In other words, the government cannot, without compelling justification, force an individual or a corporation to speak or express a particular opinion.[89]

Most notably, Apple argued that computer code should be treated as speech within the meaning of the First Amendment.[90] While a number of federal cases have held that code is speech, the Supreme Court itself has yet to rule on this argument.[91] The relevant Supreme Court precedent is unclear on whether code could count as speech for constitutional purposes.[92] Federal court cases have held that the question hinges on how *expressive* code can be.[93] If it is seen as expressive, it would be more likely to receive First Amendment protection.[94] However, if it is seen as more functional than expressive, it is less likely to be considered speech for First Amendment purposes.[95] A functional carrier or conduit of speech, such as Federal Express, would not receive protected status, but the speech itself would. Speech expresses an idea or opinion, whereas the "tools" or "conduits" of speech are mere hosts.[96] By analogy, the question is whether code is more like a typewriter, which is a technology that hosts speech, or the speech itself, like a poem typed on the machine.[97]

The existence of such a "functionality" doctrine of speech is controversial, but it may feature in a Supreme Court decision on encryption.[98] If encryption software is considered "speech" under the First Amendment, companies could argue that government cannot compel them to produce code unless there is a "legitimate and worthy interest."[99] This is a high bar for the government to meet, because they would have to show that the public interest is "legitimate" and

[88] *Id.* at 798.

[89] *Id.*

[90] Apple Inc. Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search and Opposition to Government's Motion to Compel Assistant at 32–33, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, ED No. CM 16-10 (C.D. Cal. Feb. 19, 2016).

[91] *See, e.g.*, Universal City Studios v. Corley, 273 F.3d 429, 449 (2d Cir. 2001); Junger v. Daley, 209 F.3d 481, 485 (6th Cir. 2000); 321 Studios v. Metro Goldwyn Mayer Studios, Inc., 307 F. Supp. 2d 1085, 1099–1100 (N.D. Cal. 2004); United States v. Elcom Ltd., 203 F. Supp. 2d 1111, 1126 (N.D. Cal. 2002); Bernstein v. United States Dep't of State, 922 F. Supp. 1426, 1436 (N.D. Cal. 1996).

[92] *See* Adrianna Oddo, *Being Forced to Code in the Technology Era as A Violation of the First Amendment Protection Against Compelled Speech*, 67 CATH. U.L. REV. 211 (2018) (considering how Supreme Court cases weigh on the question of computer code as speech).

[93] Bernstein v. U.S. Dep't of Justice, 176 F.3d 1132, 1141 (9th Cir. 1999) (concluding that "encryption software, in its source code form and as employed by those in the field of cryptography, must be viewed as expressive for First Amendment purposes . . . .").

[94] *Id.*

[95] *Id.*

[96] *See* Wu, *supra* note 80, at 1496 (defining conduits of speech).

[97] *Id.* at 1497.

[98] *See generally id.* at 1496 (discussing the functionality doctrine).

[99] *See* Apple Inc. Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search and Opposition to Government's Motion to Compel Assistant at 33, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, ED No. CM 16-10 (C.D. Cal. Feb. 19, 2016) (noting that Apple argued that the government did not meet this standard: "Apple does not question the government's legitimate and worthy interest in investigating and prosecuting terrorists, but here the government has produced nothing more than speculation that this iPhone might contain potentially relevant information.").

"worthy" enough to overcome the presumption against regulating speech.[100] Since this is a high bar, many government interests would fail under this level of scrutiny.[101] If they fail, they cannot constitutionally carry out their desired government action.[102] As such, the First Amendment curtails government power in regulating speech. The merits of these arguments will be discussed in subsection 2.

Apple's second argument before the court was that the government's action was viewpoint discriminatory. "Viewpoint discrimination" is a term the Supreme Court has used to describe any laws or government decisions that disfavor a particular opinion in political controversy.[103] The animating principle behind this is that the government should have no power to restrict expression because of its message or ideas.[104] As such, any law or government action that is viewpoint discriminatory is presumed unconstitutional and thus invalidated by a reviewing court.[105] On this basis, the Supreme Court has even struck down a law that forbids "disparaging" speech, illustrating that even the most offensive speech is protected under the First Amendment. [106] It is a bedrock principle of First Amendment jurisprudence that "speech may not be banned on the ground that it expresses ideas that offend." [107] In short, the U.S. may not ban speech merely because it is controversial, hateful, or disagreeable.

Apple's constitutional argument that the government's order amounts to viewpoint discrimination poses a different question about the nature of code.[108] In particular, it asks whether the *use* of encryption is itself a political statement or an exercise of free speech.[109] Apple argued that when it added encryption to its operating system, "it wrote code that announced the value it placed on data security and the privacy of citizens by omitting a back door that bad actors might exploit."[110] As such, Apple apparently argues that the mere use of encryption is an exercise of politically-charged speech.[111] In its brief, Apple argued that the

[100] *Id.*

[101] *Id.*

[102] *Id.*

[103] *See generally* Joseph Blocher, *Viewpoint Neutrality and Government Speech*, 52 B.C. L. REV. 695 (2011) (discussing viewpoint discrimination).

[104] *Id.*

[105] *See id.* at 731 ("Some Supreme Court justices have focused on effect, arguing, for example, that a content-based restriction should be unconstitutional 'regardless of the motivation that lies behind it.'").

[106] Matal v. Tam, 137 S. Ct. 1744, 1765 (2017).

[107] *Id.* (striking down a trademark law forbidding the registration of trademarks that "disparage" persons, institutions, or beliefs).

[108] Apple Inc. Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search and Opposition to Government's Motion to Compel Assistant, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, ED No. CM 16-10 (C.D. Cal. Feb. 19, 2016).

[109] *Id.*

[110] *Id.* at 33–34 (*citing* Members of City Council v. Taxpayers for Vincent, 466 U.S. 789, 804 (1984)).

[111] *See id.* at 33 (*citing Members of City Council*, 477 U.S. at 804) ("The government disagrees with this position and asks this Court to compel Apple to write new software that advances its contrary views. This is, in every sense of the term, viewpoint discrimination that violates the First Amendment.").

government disagreed with this privacy-centric position and compelled Apple to write new code in order to advance its contrary views.[112]

This constitutional argument could be stronger or weaker depending on the framing. The "viewpoint" allegedly discriminated against could be defined either as the content of the encryption code itself or the use of the code in the first place.[113] This subtle difference could change the First Amendment analysis. The *use* of encryption code could be seen as a political statement, but that would be different than arguing that the encryption code *itself* is somehow expressive.[114] Since encryption code is designed to scramble language in order to make it illegible, one could argue that the purpose of encryption code is precisely anti-expressive.[115] Moreover, the code itself amounts to a series of mathematical instructions meant to direct a computer's action.[116] This could be read as quite different than traditional forms of "speech." However, it may be easier to argue that the *use* of encryption code is a political statement in itself. Since privacy is a coveted political value, the use of encryption by a private corporation could be read as a political statement enshrining privacy and decrying surveillance.[117] Accordingly, the framing of this "viewpoint discrimination" argument may determine whether encryption is ultimately regarded as speech under the U.S. Constitution.

2. The Merits and Flaws of the Code as Speech Argument: Not All Code is Created Equal

The Supreme Court has counted many kinds of expressive activities as "speech" that merit protection under the First Amendment: political donations,[118] flag burning,[119] video games,[120] and nude dancing.[121] Under case

[112] The leading example of viewpoint discrimination in U.S. case law is *Am. Booksellers Ass'n. v. Hudnut*. 771 F.2d 323 (7th Cir. 1985). In that case, Judge Easterbrook struck down an ordinance as unconstitutional because it defined pornography as a practice that featured the "graphic sexually explicit subordination of women" where women are featured in scenarios of degradation or humiliation. *Id.* at 324. This ordinance was struck down as an example of unconstitutional viewpoint discrimination. *Id.* at 332. The idea here is that the government should not be able to ban pornography (a type of speech) just because it finds it offensive. *Id.* However, there are some exceptions to this principle in the First Amendment jurisprudence, particularly related to child pornography.

[113] Blocher, *supra* note 103, at 729–31.

[114] *Id.*

[115] While the product of the code may be anti-expressive, the code itself and the manner of encryption may still express the style and personality of the coder. This could be another way in which code is expressive for First Amendment purposes.

[116] *Introduction to Code*, STAN. U., https://web.stanford.edu/class/cs101/code-1-introduction.html (last visited Mar. 10, 2019).

[117] Marco Kuhnel et al., *Encryption From A Human Rights Perspective*, U.N. OFF. HIGH COMM'R HUM. RTS., https://www.ohchr.org/Documents/Issues/Opinion/Communications/MarcoKuhnel.pdf; Rainey Reitman, *Amnesty International: Encryption is a Human Rights Issue*, ELEC. FRONTIER FOUND. (Mar. 31, 2016), https://www.eff.org/deeplinks/2016/03/amnesty-international-encryption-human-rights-issue.

[118] Citizens United v. FEC, 558 U.S. 310, 372 (2010) (holding freedom of speech prohibits government from restricting political expenditures by nonprofits, corporations, labor unions, and other associations).

[119] Texas v. Johnson, 491 U.S. 397, 420 (1989).

[120] Brown v. Entm't Merch. Ass'n, 564 U.S. 786, 805 (2011).

[121] Barnes v. Glen Theatre, Inc., 501 U.S. 560, 572 (1991) (holding that while nude dancing is expressive conduct under the First Amendment, the government's interest in societal order was compelling enough to justify its regulation).

law in lower courts, a "Like" on Facebook has also been deemed an exercise of free speech.[122] Two federal courts have even held that encryption code was sufficiently expressive for First Amendment protection.[123] To reiterate, deeming an activity protected speech means that a government regulation could have to pass a higher constitutional bar by showing a compelling government need.[124] Otherwise, a court would strike it down as unconstitutional.[125] An expansive view of the First Amendment that includes code would mean that code would be more difficult to regulate.[126] With this concern in mind, the argument that code should be constitutionally protected speech is seen by some as unconvincing.[127] The argument of code as speech put forth by Apple is likely to recur in future technology cases and merits a nuanced evaluation. The main problem with the idea of code as speech is that it does not consider the variety in types of computer code.

Some types of code can have the expressive qualities of speech, while others are purely functional mathematical equations.[128] Regulations of some outputs of code, like the content of websites or video games, have already been deemed by the Supreme Court as worthy of First Amendment treatment.[129] Indeed, algorithms in decision-making software sometimes express the opinions, judgments, or biases of the creators.[130] Since coding involves creative human judgment, even racial biases can be baked into the code itself.[131] For instance, one kind of commercial software developed to determine whether particular convicts should receive probation was more likely to incorrectly label a black person as "high risk" than a white person.[132] Facial recognition algorithms have also been shown to fail at recognizing non-white faces.[133] The presence of biases and opinions in code shows that it can be more than purely functional and is in fact expressive or "speech-like."[134] On the other hand, many other types of code are not expressive at all.[135] Back-end code, which users

[122] Bland v. Roberts, 730 F.3d 368, 394 (4th Cir. 2013).

[123] Junger v. Daley, 209 F.3d 481, 485 (6th Cir. 2000); Bernstein v. U.S. Dep't of Just., 176 F.3d 1132, 1145 (9th Cir. 1999).

[124] *See supra* notes 118–23 (discussing this analysis).

[125] Citizens United v. FEC, 558 U.S. 310, 340 (2010).

[126] Benjamin, *supra* note 80, at 1448.

[127] *See* Wu, *supra* note 80, at 1526–27 (explaining that Google's rankings of webpage should not be protected by the First Amendment); *cf*. Benjamin, *supra* note 80, at 1445.

[128] Wu, *supra* note 80, at 1513–14.

[129] *See* Brown v. Entm't Merch. Ass'n, 564 U.S. 786, 805 (2011) (holding that law prohibiting the sale or rental of "violent video games" to minors violated the First Amendment); Neil Richards, *Apple's Code = Speech Mistake*, MIT TECH. REV. (Mar. 1, 2016), https://www.technologyreview.com/s/600916/ apples-code-speech-mistake.

[130] Julia Angwin et al., *Machine Bias*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

[131] *Id.*

[132] Angwin et al., *supra* note 130; *see also* CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY (Crown Pub. Grp. 2016) (discussing the harms caused by big data).

[133] Joy Buolamwini, *How I'm Fighting Bias in Algorithms*, TED.COM (Nov. 2016), https://www.ted.com/talks/joy_buolamwini_how_i_m_fighting_bias_in_algorithms/transcript?language=en.

[134] *See supra* notes 129–33 (showing bias in some decision-making algorithms).

[135] *See, e.g.*, Wu, *supra* note 80, at 1524–26 (explaining that car alarms, antilock braking systems, and map programs are not speech protected by the First Amendment).

never interact with, can be purely functional.[136] The code used for anti-virus software is another example of potentially non-expressive code.[137] Nevertheless, the level of functionality in code is not a dispositive factor in determining whether it receives First Amendment protection.[138] According to the federal court in *Bernstein v. United States*, the presence of "one drop of direct functionality" does not overwhelm "any constitutional protections that expression might otherwise enjoy."[139] This means that the functional aspects of code should not alone preclude it from receiving First Amendment protection.[140]

Some forms of code thus contain elements of speech *and* non-speech.[141] While the Supreme Court has never officially recognized this, the U.S. Court of Appeals for the Second Circuit recognized that computer code and computer programs are forms of speech covered by the First Amendment in *Universal City Studios, Inc. v. Corley*.[142] Acknowledging the functionality doctrine described above, the Second Circuit held that a computer program contains both speech and non-speech components.[143] According to the court, the fact that the encoded information is ultimately transferred to a computer rather than a human does not make a difference:

> Computer programs are not exempted from the category of First Amendment speech simply because their instructions require use of a computer. *A recipe is no less "speech" because it calls for the use of an oven and a musical score is no less "speech" because it specifies performance on an electric guitar*. Arguably distinguishing computer programs from conventional language instructions is the fact that programs are executable on a computer.[144]

The focal point of the court's analysis was that in order to be speech, the "instructions" or "recipe" must convey information.[145] Whether it is executed by a human or a computer is immaterial for First Amendment purposes.[146] The aspect of conveying information is particularly important for the analysis of whether encryption code, in particular, qualifies as speech.[147] Unlike any other

[136] *See* Brown v. Entm't Merch. Ass'n, 564 U.S. 786, 790 (2011) ("[V]ideo games communicate ideas . . . through features distinctive to the medium (such as the player's interaction with the virtual world). That suffices to confer First Amendment protection.").

[137] *See* Meiring de Villiers, *Opinionated Software*, 10 VAND. J. ENT. & TECH. L. 269, 272 ("A virus alert, as a statement on an issue of great public concern, merits protection under the First Amendment.").

[138] Wu, *supra* note 80, at 1517 (arguing that functionality will usually be the line dividing speech and communications when it comes to algorithmic output, absent suspicious censorial motives).

[139] Bernstein v. U.S. Dept. of Justice, 176 F.3d 1132, 1142 (9th Cir. 1999).

[140] *Id.*

[141] *See* Universal City Studios, Inc. v. Corley, 273 F.3d 429, 451 (2d Cir. 2001) (recognizing that computer codes have both speech and nonspeech components).

[142] *Id.* at 449–50.

[143] *Id.* at 451.

[144] *Id.* at 447 (emphasis added); *see also* ASHLEY PACKARD, DIGITAL MEDIA LAW (Wiley-Blackwell 2d ed., 2013).

[145] *Corley*, 273 F.3d at 447 ("[I]t is the conveying of information that renders instructions 'speech' for purposes of the First Amendment."); AARON SCHWABACH, INTERNET AND THE LAW: TECHNOLOGY, SOCIETY AND COMPROMISES (2d ed. 2014).

[146] SCHWABACH, *supra* note 145.

[147] *See, e.g.*, Colangelo & Maurushat, *supra* note 80, at 74–78 (2006) (exploring encryption code's expressive nature by discussing a trilogy of encryption export cases).

type of code, its end goal is to make information inaccessible.[148] Then again, the code itself could be expressive because encryption code can be written in a variety of different ways, reflecting the styles and preferences of the writer.[149] By analogy, a recipe can be expressive because it contains the judgment and preferences of the chef. While mixing could be achieved by shaking or stirring, the choice between those two is personal.[150] Similar judgment calls can be made in coding that may make it more expressive than it appears.

One contribution of this Article is the argument that not all code is created equal and constitutional jurisprudence should treat different kinds of code differently. This is the main problem with the First Amendment argument that code should be treated as speech. It does not account for the variety in functionality and expression present in different kinds of code. Google's search results algorithm is not the same as encryption code, which is not the same as the code used to create a video game. Encryption code is more likely to be purely functional rather than expressive.[151] As mentioned earlier, the purpose of encryption is to scramble information, rather than express it.[152] While the content of encrypted communications may be speech, it is harder to argue that the encryption code itself amounts to protected speech.

The question of whether a particular activity should receive First Amendment protection often turns on the question of whether it qualifies as speech. However, an analysis of the *purpose* of the First Amendment could yield different results. As Neil Richards notes, "[w]hat matters in the end, isn't the metaphysics of 'speechiness,' but whether a government regulation of an activity threatens the traditional values of free expression—political dissent, art, philosophy, and the practices of self-government."[153] Richards suggests that equating code with speech would lead to an excessive expansion of First Amendment protection.[154] This would have the effect of largely insulating all code from regulation, he argues.[155] Indeed, a conclusion that *all* code is speech would expand First Amendment protection in counter-intuitive ways.[156] It risks treating "code for a malicious virus as equivalent to writing an editorial in the *New York Times*."[157] But this problem could be solved by differentiating between types of code and subjecting each to its own legal analysis.

Arguments based on the purpose of an Amendment or statute are typically given less weight due to their malleability. But under a purposivist analysis of the First Amendment, encryption technologies could be justified on the basis

[148] *Id.* at 73.

[149] *See id.* at 75 (explaining that cryptographers could use source code to express idea).

[150] E-mail from Rebecca Williams to Olivia Gonzalez (Jun. 25, 2017) (email on file with author).

[151] *See* Colangelo & Maurushat, *supra* note 80, at 77 (explaining that encryption code is inherently functional).

[152] Blocher, *supra* note 103, at 729–31.

[153] Richards, *supra* note 129.

[154] *Id.*

[155] *Id.*

[156] *See id.* ("[T]here are many things that humans will do with code that will have nothing to do with the First Amendment . . . .").

[157] *See id.* (explaining the difficulties in treating code as speech).

that they uniquely protect free speech.[158] Indeed, this is the main argument for strong encryption in international human rights law.[159] According to the Report by UN Special Rapporteur David Kaye, "encryption and anonymity enable individuals to exercise their rights to freedom of opinion and expression in the digital age and, as such, deserve strong protection."[160] A related, purpose-driven argument could be made about the role of encryption in free speech under the First Amendment.[161] It is worth nothing that this is a different kind of argument, relying on arguments about the *purpose* of the First Amendment rather than the existing understanding of the text.[162]

Under this argument, the purpose of the First Amendment is to prevent government regulations that threaten free expression.[163] The weakening of encryption technologies could produce a chilling effect if users feel their communications are not private or secure.[164] If the chilling effect is great enough to stifle the free exchange of ideas, the weakening of encryption could threaten First Amendment values.[165] As such, a purposivist approach to the First Amendment would provide some argument for the preservation of strong encryption.[166] While it has some pragmatic appeal, a purposivist argument alone is probably insufficient to strike down a government regulation mandating encryption back doors.[167]

In short, different types of code merit their own distinctive legal treatment. Encryption and algorithmic decision making are not the same, and there is a spectrum of expressiveness in code.[168] The section above showed why the "code

[158] *See generally* Patrick I. Ross, *Computer Programming Language: Bernstein v. United States Department of State*, 13 BERKELEY TECH. L.J. 405, 415–16 (1998) (concluding that whether computer source code is constitutionally protected free speech and whether export controls on cryptography are unconstitutional requires a detailed factual analysis).

[159] *See* Kaye, *supra* note 35 (giving an example of an argument why there is a need for strong encryption in international human rights law).

[160] *Id.*

[161] *See generally* E. John Park, *Protecting the Core Values of the First Amendment in an Age of New Technologies: Scientific Expression vs. National Security*, 2 VA. J.L. & TECH. 3 (1997) (discussing an example of a purpose-driven argument about why encryption should be afforded First Amendment protections).

[162] *See generally* Richard A. Posner, *Pragmatism Versus Purposivism in First Amendment Analysis*, 54 STAN. L. REV. 737 (2002) (explaining the differences between pragmatist and purposivist arguments about the First Amendment).

[163] *Id.* at 743–44.

[164] As mentioned in the introduction of this Article, a "chilling effect" is an over-deterrence of valuable speech. The Supreme Court has relied on this concept in its First Amendment jurisprudence and recognized its duty to "insulate all individuals from the chilling effect upon exercise of First Amendment freedoms." Walker v. City of Birmingham, 388 U.S. 307, 345 (1967) (Brennan J., dissenting). The Court's goal here was to give the freedoms the necessary "breathing space to survive." *Id.* at 345.

[165] *Id.*

[166] *See generally* Lee Tien, *Publishing Software as a Speech Act*, 15 BERKELEY TECH. L.J. 629 (2000) (analyzing the *Bernstein* case and whether computer programs written in source code can be a form of expression for purposes of the First Amendment).

[167] *See generally* Shannon Lear, *The Fight over Encryption: Reasons Why Congress Must Block the Government from Compelling Technology Companies to Create Backdoors into Their Devices*, 66 CLEV. ST. L. REV. 443, 445 (2018) (explaining the various policy considerations surrounding encryption backdoors).

[168] *See generally* Soheila Omer Al Faroog Mohammed Koko et al., *Comparison of Various Encryption Algorithms and Techniques for Improving Secured Data Communication*, 17 IOSR J. COMPUT. ENG'G 62 (2015) (explaining the differences between different data encryption and communication methods); *see also* Saranya Vijayakumar, *Algorithmic Decision-making*, HARV. POL. REV. (June 28, 2017), http://harvardpolitics.com/covers/algorithmic-decision-making-to-what-extent-should-computers-make-decisions-for-society; Christina

as speech" argument underlying Apple's compelled speech and viewpoint discrimination arguments is flawed, though its principles may have some application in future cases. The exact weight to each interest is balanced on the normative considerations a court would consider. The following section will explain the policy effects of viewing code as speech. It will explain which stakeholders (government, corporate, or civil society) are harmed and benefited if encryption is considered speech.

3. *Policy Ramifications of Code as Speech*

The understanding of code as speech has concrete policy ramifications for the stakeholders involved. Government would have less regulatory power over technology companies if code received First Amendment protection.[169] A government action mandating encryption back doors would be less likely to survive judicial review.[170] This would benefit companies financially because the increased network security of strong encryption could save them compliance and litigation costs caused by security breaches.[171] The perception of these companies as secure could also benefit them financially if consumers value security in their product choices.[172]

Even if security and privacy make no difference in consumer choices, the absence of back doors could still be beneficial for national economies.[173] If the information systems underlying U.S. companies are seen as secure, global investors will have reason to back U.S. companies.[174] For example, a bank might be less likely to host its information on servers or products that do not use strong encryption.[175] If the bank's risk analysts calculate that the costs of a potential data breach are high enough, it may be rational for a bank to refrain from hosting information without encryption.[176] If the U.K. bans encryption, companies may reason similarly and refrain from incorporating or operating in

Mercer, *What Is Encryption*?, TECHWORLD (May 15, 2018), https://www.techworld.com/security/what-is-encryption-3659671.

[169] *See generally* FREEDOM F. INST., *supra* note 81 (showing that unless code is explicitly added to the enumerated list of unprotected speech under the First Amendment, it is harder for the government to regulate that speech).

[170] *Id.*

[171] While it is possible that privacy and security concerns have no effect on consumer behavior, some studies have noted that trust does play a role in consumer choice. *See, e.g.*, Ramnath K. Chellappa & Raymond G. Sin, *Personalization Versus Privacy: An Empirical Examination of the Online Consumer's Dilemma*, 6 INFO. TECH. MGMT. 181 (2005). For more general discussion on the impact of privacy, see Thomas M. Lenard & Paul Rubin, *In Defense of Data: Information and the Costs of Privacy*, TECH. POL'Y INST. (2009).

[172] While it is possible that privacy and security concerns have no effect on consumer behavior, some studies have noted that trust does play a role in consumer choice. *See, e.g.*, Chellappa & Sin, *supra* note 171 (providing an example of such a study). For more general discussion on the impact of privacy, see Lenard & Rubin, *supra* note 171.

[173] Todd Bell, *The Economics of Back Doors: Why It's Bad for U.S. Corporations and the U.S. Economy*, CSO (Feb. 24, 2016, 1:24 PM), https://www.csoonline.com/article/3036779/security/the-economics-of-backdoors.html.

[174] *Id.*

[175] *Id.*

[176] *Id.*

the U.K.[177] This would pull investment and business away from countries with legislative burdens on encryption.[178] The cyber security risk may only be one component of a business' decision to operate in a particular country. However, it is a heavy enough factor that legislators should consider the impact of encryption bans on the national economy.

Consumers and civil society would also benefit from increased privacy and civil liberties. Strong encryption would mean that consumers could exchange ideas freely and host their information on digital devices with confidence that it would not be compromised by a bad actor exploiting a back door.[179] One way in which civil society might be harmed is that a legal interpretation of *all* code as speech would mean a drastic deregulation of code.[180] This would include types of code that perhaps should be regulated, such as discriminatory algorithms.[181] Extending First Amendment protection to code may prevent the government from mandating back doors, but it could also restrain the government excessively.[182] A narrower approach might be necessary in which only some types of code are viewed as speech.

The government would be most harmed by a legal regime which recognizes code as speech and therefore prevents mandated back doors.[183] Encrypted communications would make law enforcement investigations more difficult.[184] The government could not, as it sought to do in the Apple-FBI case, compel a private company to incorporate back doors.[185] Moreover, the implementation of end-to-end encryption means that law enforcement could not immediately access the contents of encrypted communications.[186] At first glance, this would change the nature of national security investigations. However, as Orin Kerr notes, there are a variety of "encryption workarounds" that can be used if strong

[177] *See generally* Alex Hern, *UK Government Can Force Encryption Removal, But Fears Losing, Experts Say*, THE GUARDIAN (Mar. 29, 2017, 3:30 PM), https://www.theguardian.com/technology/2017/mar/29/uk-government-encryption-whatsapp-investigatory-powers-act (exploring the risks inherent in the U.K. government's proposed ban on encryption).

[178] *Id.*

[179] *See generally* Andi Wilson Thompson, *The Human Rights Benefits of Encryption*, NEW AM. (Mar. 2, 2015), https://www.newamerica.org/oti/blog/the-human-rights-benefits-of-encryption (explaining the human rights benefits to encouraging wider use of encryption).

[180] *See generally* Gabriella Coleman, *Code Is Speech: Legal Tinkering, Expertise, and Protest Among Free and Open Source Software Developers*, 24 CULTURAL ANTHROPOLOGY 420 (2009) (explaining the different dimensions of the arguments surrounding whether all code should be considered speech).

[181] *See generally id.* (discussing the different categorization of code in regard to speech).

[182] *See generally id.* (exploring the legal arguments surrounding the question of whether code should be considered speech).

[183] *See generally* David Ruiz, *The Secure Data Act Would Stop Backdoors*, ELEC. FRONTIER FOUND. (May 10, 2018), https://www.eff.org/deeplinks/2018/05/secure-data-act-would-stop-backdoors (giving one example of a bill in Congress that would eliminate all government backdoors into encrypted software).

[184] *See generally Should Law Enforcement Have the Ability to Access Encrypted Communications?*, WALL ST. J. (Apr. 19, 2015 11:11 PM), https://www.wsj.com/articles/should-law-enforcement-have-the-ability-to-access-encrypted-communications-1429499474 (exploring the debate over whether law enforcement agencies should have access to encrypted communications).

[185] *See generally* Alina Selyukh, *A Year After San Bernardino And Apple-FBI, Where Are We On Encryption?*, NPR (Dec. 3, 2016, 1:00 PM), https://www.npr.org/sections/alltechconsidered/2016/12/03/504130977/a-year-after-san-bernardino-and-apple-fbi-where-are-we-on-encryption (giving a general overview of the Apple-FBI encryption debate).

[186] *Id.*

encryption is maintained.[187] The government would not receive its preferred method of investigation in certain cases, but it could still conduct its law enforcement efforts.[188] Indeed, the government may still use other methods to access the plaintext of an encrypted communication.[189] These encryption workarounds will be discussed in greater detail in Part B.

If strong encryption were protected, one group that would benefit is the privacy and civil liberties community.[190] If end-to-end encryption is preserved on speech grounds, the civil liberties community may feel more secure that the government could not use arguments of national security to pass a regulation or compel a company to decrypt information.[191] A government regulation would have to pass a high level of judicial scrutiny that, as mentioned above, would present a considerable obstacle.[192] This produces favorable results for civil liberties advocates concerned about the government's ability to conduct surveillance.[193]

Finally, it is also important to consider the policy ramifications of how the judicial system would be affected. An expansion of First Amendment protection here means that courts would get increasingly involved in the definition of code.[194] This is not necessarily in the public interest, particularly if issues of technology are better settled in the legislature.[195] Courts could promulgate inconsistent definitions of code and create a more muddled legal doctrine.[196] Moreover, the legislature is frequently better equipped with experts to legislate on technical issues such as encryption.[197] On the other hand, the introduction of this Article explained that courts might be *better* suited to resolving these cases because a legislative one-size-fits-all solution could never be sufficient.[198] According to Lawrence Lessig, courts should rule on these issues and "translate" existing constitutional principles so that we don't bend our precedent out of shape.[199] Cass Sunstein, by contrast, thinks that courts should stay out of this because technology changes too quickly.[200] Indeed, encryption could change with advances in technology like quantum computing. Quantum computing

[187] Kerr & Schneier, *supra* note 49, at 991.

[188] *Id.*

[189] *See infra* Part B(2) (exploring "encryption workarounds").

[190] *See* Coleman, *supra* note 180 (explaining the benefits to civil liberties from strong encryption policies).

[191] *See generally* 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?utm_term=.7f4cf8edd149 (explaining arguments about why the government should be able to require tech companies to give the government access to encrypted data).

[192] *See infra* Part I (a)(1) (exploring the level of judicial scrutiny that would be applied to any such law).

[193] *See* Coleman, *supra* note 180 (exploring the benefits to civil liberties from strong encryption policies).

[194] *See generally id.* (exploring the legal ramifications of the courts defining what counts as "code" in terms of the First Amendment).

[195] *Id.*

[196] *Id.*

[197] For further discussion on the capability of courts to deal with encryption and technology cases, see Jonathan Mayer, *Government Hacking*, 127 YALE L.J. 570, 609–14 (2018).

[198] *Id.*

[199] Lessig, *supra* note 74, at 873.

[200] Sunstein I, *supra* note 63, at 292.

could strengthen encryption even further, making the mathematical puzzle underlying modern encryption even more difficult to crack.[201] It could also fundamentally change the nature of encryption in material ways that may not yet be apparent. The research on this is still developing, but such advances make it difficult for courts to promulgate rules that will have future applications. Given rapid technological change, judges may be caught in a game of legal whack-a-mole, seeking to regulate an increasingly elusive target. These factors are relevant in our consideration of whether to approach encryption as a constitutional question to be settled by courts or as a question of pure policy to be handled by the legislature.

The First Amendment is not the only legal framework in the U.S. where encryption might fit. Encryption can be thought of as a kind of speech or as a mechanism for protecting free speech, but it can also be examined through a prism of government investigatory power. The Apple-FBI case shows that encryption is only problematic for government interests because it makes criminal investigations more complicated. The Fourth Amendment of the U.S. Constitution is the primary authority controlling the use of search warrants and government investigatory power. The following section examines encryption through this lens.

B. Fourth Amendment Approaches: Warrants, Searches, and Government Power

While the Fourth Amendment implicitly protects an individual right to privacy, it does so by limiting the government's investigatory power. The Fourth Amendment provides for a right of "people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[202] As Jonathan Mayer notes, courts have shaped this textual command into a "framework of information privacy law."[203] The cornerstone of this doctrine is the question of whether a particular government action constitutes a "search" under the Fourth Amendment. If it is considered a search under the Fourth Amendment, the government must show probable cause and obtain a search warrant in order to conduct it. The search question is thus the "gatekeeper for constitutional surveillance regulation."[204]

Searching a person's home is a classic example of a Fourth Amendment search, typically requiring a warrant. However, the definition of a search becomes less clear in the context of electronic communications and personal data. The U.S. Supreme Court has shed light on the matter in a number of cases. In *United States v. Jones*, the Supreme Court held that installing a GPS tracking

[201] For a layman's introduction to quantum cryptography, see Adam Mann, *Laws of Physics Say Quantum Cryptography is Unhackable. It's Not.*, WIRED (June 7, 2013), https://www.wired.com/2013/06/quantum-cryptography-hack (explaining that in quantum cryptography the "key is encrypted into a series of photons that get passed between two parties trying to share secret information. The Heisenberg Uncertainty Principle dictates that an adversary can't look at these photons without changing or destroying them.").

[202] U.S. CONST. amend. IV.

[203] Mayer, *supra* note 197, at 581.

[204] *Id.*

device on a vehicle to monitor its movements constituted a search.[205] Famously, in *Katz v. United States*, the Supreme Court found that the FBI had conducted a search when it used an electronic eavesdropping device to catch Charles Katz discussing illegal gambling wagers on a public pay phone.[206] In *Florida v. Jardines*, the Court held that police use of a trained dog to sniff for narcotics outside a private residence constituted a search.[207] In order to determine whether something constitutes a search, the court asks whether the individual had a "reasonable expectation of privacy."[208] Most pertinently, *Riley v. California* held that the police generally may not, without a warrant, search digital information on a cell phone seized from an individual who has been arrested.[209] The fact that something qualifies as a Fourth Amendment search does not mean that the government cannot conduct the search, only that a warrant would be necessary. The warrant, granted by a judge, acts as a protection of an individual's constitutional right to privacy. It requires the government to justify its invasion of privacy in order for a search to be valid.

Encryption's place in this constitutional landscape remains unclear. In the Apple-FBI dispute, Fourth Amendment questions about government investigatory powers were not raised because the government did acquire a warrant to access the terrorist's iPhone. As a result, no analysis on the validity of the search was needed. Nevertheless, future cases could pose questions about encryption's place in this constitutional framework. In particular, proposed regulatory frameworks mandating back doors could be challenged. Additionally, the government's use of "lawful hacking" or "workarounds" to obtain encrypted communications may also give rise to Fourth Amendment questions. The following subsections will address how Fourth Amendment doctrine might respond to these pressures, paying particular attention to the policy effects of each legal approach.

More generally, these subsections reflect the evolving definition of government investigatory power and the philosophical underpinnings of privacy. These notions have been baked into the Fourth Amendment since its inception in the 1770s.[210] Encryption joins the list of modern phenomena that unfasten the idea of a government "search" from the *physical* bounds of an individual's "person, house, papers," or belongings.[211] It creates a more complex picture of privacy which includes an individual's electronic data.

[205] 565 U.S. 400, 431 (2012).

[206] 389 U.S. 347, 359 (1967).

[207] 569 U.S. 1, 15–16 (2013).

[208] *Id.* at 10.

[209] 573 U.S. 373, 403 (2014).

[210] *See generally* Christopher Slobogin, *A Defense of Privacy as the Central Value Protected by the Fourth Amendment*, 48 TEX. TECH. L. REV. 143 (2015) (explaining the origins of the notion of privacy in the Fourth Amendment).

[211] U.S. CONST. amend. IV.

1. Regulatory Challenges: Encryption and the Reasonable Expectation of Privacy

A U.S. law on encryption cannot be passed if it conflicts with the constitutional framework explained above.[212] In particular, a law that grants the government warrantless access to back doors could be unconstitutional under the Fourth Amendment.[213] As Orin Kerr points out, "the privacy implications of encryption have led many Internet law scholars to declare encryption regulation constitutionally off-limits."[214] The interpretation of this constitutional doctrine could determine the regulation of encryption, shaping it in ways that will have meaningful policy repercussions.

Under the Fourth Amendment, the government must obtain a warrant when the individual searched has a "reasonable expectation of privacy."[215] This means that if an individual would reasonably expect the contents of the search to remain private, a warrant is necessary for law enforcement to invade that private space.[216] For example, the Supreme Court has held that a person has a "reasonable expectation of privacy" in the contents of a sealed package, making the intrusion a search requiring a warrant.[217] Similarly, Fourth Amendment protection over encrypted communications turns on whether the encryption creates this reasonable expectation of privacy.[218] If so, the Fourth Amendment requires that the government obtain a warrant before decrypting or exploiting a back door to those communications.[219]

According to Supreme Court doctrine, one way of determining whether there was a reasonable expectation of privacy is by examining whether the information in question was disclosed to a third party.[220] The rationale here is that if an individual disclosed the information to a third party, they did not expect

[212] Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?"*, 33 CONN. L. REV. 503, 504 (2001) [hereinafter Kerr II].

[213] *Id.*

[214] *Id.*

[215] *See* Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) (noting the Fourth Amendment protections with respect to the reasonable expectation of privacy).

[216] Orin Kerr argues that encryption *cannot* create this expectation because the Fourth Amendment "regulates government *access* to communications, not the *cognitive understanding*" of communications already obtained." Kerr II, *supra* note 212, at 504 (emphasis added). By contrast, David Allan Jordan points out that this argument presupposes that the information in the government's hands was acquired pursuant to a warrant or constitutionally permissible means. *See* David Alan Jordan, *Decrypting the Fourth Amendment: Warrantless NSA Surveillance and the Enhanced Expectation of Privacy Provided by Encrypted Voice Over Protocol*, 47 B.C. L. REV. 505, 538 (2006) (discussing the proposed change to NSA guidelines to prevent the dissemination of information gained through the frustration of the reasonable expectation of privacy). In other words, under Professor Kerr's understanding the government would be free to do what it pleases with data collected through a warrantless surveillance program because once the data was lawfully in the possession of the government, the Fourth Amendment protections could not be triggered.

[217] *See, e.g.*, United States v. Chadwick, 433 U.S. 1, 11 (1977) ("By placing personal effects inside a doublelocked footlocker, respondents manifested an expectation that the contents would remain free from public examination."); *see also* Mayer, *supra* note 197, at 590 (discussing the reasonable expectation of privacy for the contents of a sealed package).

[218] Riley v. California, 573 U.S. 373, 403 (2014); *The Fourth Amendment in Cyberspace*, *supra* note 212, at 504–05.

[219] *See generally Carpenter*, 138 S. Ct. at 2222 (discussing Fourth Amendment limitations).

[220] Kerr II, *supra* note 212, at 511.

it to remain private.[221] For example, in *Katz v. United States*, the Court reasoned that a collection of dialed phone numbers (a pen register) did not constitute a search because it was voluntarily disclosed to the telephone company.[222] The telephone company was considered to be the third party to which the caller disclosed the information.[223] As a result, the Court held that there was no reasonable expectation for the information to remain private.[224]

Katz thus illustrates two principles that are important for the application of Fourth Amendment jurisprudence to encryption. The first is the Third Party Doctrine articulated above, which states that anything disclosed to a third party cannot receive Fourth Amendment protection because there is no "reasonable expectation of privacy."[225] This is important for encryption because end-to-end encryption is used precisely so that the communications are not accessible to third parties.[226] By definition, strong encryption means that the encryption key is not even disclosed to the platform hosts, like Apple or WhatsApp.[227] If keys were retained, a court could find that the contents of conversations would be, in fact, disclosed to a third party.[228] Put differently, if Apple or WhatsApp have access to a back door or encryption key, they have the technical capability to surveil the content of communications.[229] As such, a user would be less reasonable in expecting that their communications remain private.[230] With this in mind, a court could find that the information has been disclosed to a third party and thus may not receive Fourth Amendment protection.[231] Conversely, a court could find that even despite the presence of a back door, an individual still has a reasonable expectation that their communications would remain private. If a back door exists such that the government can only use it in narrow circumstances, an individual might still have a reasonable expectation of privacy in general.[232] The resolution of this question could have important implications for encryption: if a platform provider's access to back doors amounts to a third party disclosure, the government may not need a warrant to access the information.[233]

This would also depend on whether the warrant was for the content of communications or metadata. The second relevant principle articulated by *Katz* is the distinction between content and non-content.[234] By analogy, the "content"

[221] *Id.*

[222] Katz v. United States, 389 U.S. 347, 350–51 (1967).

[223] *Id.* at 349.

[224] *Id.* at 359.

[225] *Id.*

[226] Issam Andoni, *The Case for End–To–End Encryption*, FORBES (June 5, 2018), https://www.forbes.com/sites/forbestechcouncil/2018/06/05/the-case-for-end-to-end-encryption/#f07eae119acc (describing how end-to-end encryption works).

[227] *Id.*

[228] Kerr II, *supra* note 212, at 504 n.6 (discussing the potential regulatory limits on encryption).

[229] *Id.* at 529; Mayer, *supra* note 197, at 576, 585.

[230] Kerr II, *supra* note 212, at 529.

[231] This will also depend in part on whether the communication is metadata or content, a subject to be addressed later in this Article.

[232] Kerr & Schneier, *supra* note 49, at 1012; Mayer, *supra* note 197, at 597.

[233] *See* Smith v. Maryland, 442 U.S. 735, 745 (1979) (finding that government collection of dialed digits with a pen register device did not constitute a search).

[234] Katz v. United States, 389 U.S. 347, 354 (1967).

of communications would be the information inside a letter, where the non-content or metadata would be the addresses on the envelope. In *Katz*, the court ruled that the dialed digits did not comprise the *content* of a communication and thus had no reasonable expectation of privacy.[235] If the government requests the encrypted content of a communication, a warrant would generally be necessary.[236] However, if the requested information is metadata (such as the timestamp on a message), a warrant may not be necessary.[237] This is important because the possession of a warrant determines the legality of a government search.[238]

The already crude distinction between content and non-content has been further eroded by advances in technology.[239] Steven Bellovin explains that the Internet of Things, or the interconnection of computing devices and household appliances, is similarly disrupting this distinction.[240] In a networked environment where devices from "smart thermostats to pacemakers to tire pressure sensors" all communicate over the same network, notification of a communication may be the entirety of the communication.[241] This means that the message and the metadata become "one and the same."[242] Crude though this distinction might be, it remains the prevailing legal doctrine.[243] The question of whether information sought by the government is content or non-content would determine the need for a warrant.[244] As Jonathan Mayer notes, web and email metadata are categorically unprotected so "law enforcement officers may obtain it without a warrant."[245] While these distinctions may seem semantic, they have practical implications for the regulation of encryption. The manner in which existing constitutional doctrine is interpreted or changed in response to encryption technology will have important social impacts. Without a regulation requiring back doors, the government must rely on exploiting existing software vulnerabilities in order to acquire encrypted communications. The following subsection deals with the Fourth Amendment as it applies to these "lawful hacking" practices.[246]

2. *Lawful Hacking and Defining Fourth Amendment Protections*

"Lawful hacking" is the government's use of existing software vulnerabilities to access information for investigatory purposes.[247] It is

[235] *Id.* at 354.

[236] Kerr II, *supra* note 212, at 504.

[237] Bellovin, *supra* note 49, at 13; Mayer, *supra* note 197, at 596.

[238] Kerr II, *supra* note 212, at 504 (discussing the Fourth Amendment protections).

[239] *Id.*

[240] Bellovin, *supra* note 49, at 8, 11.

[241] *Id.* at 8.

[242] *Id.*

[243] *Id.*

[244] *See generally id.* (discussing the content/non-content distinction and the prevailing law).

[245] Mayer, *supra* note 197, at 602.

[246] *See generally* Bellovin, *supra* note 49 (discussing lawful hacking); Kerr & Schneier, *supra* note 49, at 1009 (discussing lawful hacking).

[247] Encryption workarounds, by contrast, are efforts to "reveal [an unencrypted] version of a target's data that has been concealed by encryption." Kerr & Schneier, *supra* note 49, at 991. The two concepts are related

considered a way of working around the encryption of communications.[248] As such, it is presented as an alternative to mandated back doors.[249] For instance, if an encrypted email chain were uploaded to an unencrypted Cloud service, one low-tech form of lawful hacking would be for the government to acquire the backed up version on the Cloud.[250] Lawful hacking can range in technological complexity and often uses many techniques implemented by ordinary hackers, such as spear-phishing.[251] In a number of investigations, law enforcement agents have used a "watering hole strategy" whereby they take over the operation of a website and deliver surveillance malware to users when they log in.[252] Accordingly, the watering hole strategies target individuals who engage in specific suspicious behaviors.[253] These are only some types of lawful hacking or "government malware" strategies.[254] Law enforcement may also seize a device to conduct a hack, as they did in the Apple-F.B.I. case.[255] Overall, lawful hacking is seen as an alternative response to mandating encryption back doors.[256] The rationale is that law enforcement can access the information it needs without mandating network insecurity through back doors.[257]

Whether the government's use of lawful hacking triggers Fourth Amendment protections depends on the type of hacking and the type of Fourth Amendment interpretation taken. Jonathan Mayer frames the doctrinal analysis in the previous subsection slightly differently, noting two different conceptions of information privacy under the Fourth Amendment.[258] The first conception sees the Fourth Amendment as protecting the integrity of *devices* and the second as protecting *information*.[259] Under the device-centric conception, lawful hacking falls into the Fourth Amendment's purview.[260] This is because the government breaking into a computer is analogous to functionally "cracking open a closed container."[261] The reasoning is that if the Constitution protects the integrity of private spaces, it also protects devices like computers and smartphones.[262] Under this understanding, any kind of lawful hacking by the government would require a warrant.[263]

but not necessarily the same. As Kerr and Schneier explain, encryption workarounds can include things like accessing a plaintext copy of the communications while it is opened by the user. *Id.* This could be as low-tech as obtaining a screenshot of communications from an informant. While lawful hacking is one type of encryption workaround, it does not represent the full gambit of investigatory options available to law enforcement. *Id.* at 992.

[248] Bellovin, *supra* note 49, at 7–9; Kerr & Schneier, *supra* note 49, at 1006.

[249] Bellovin, *supra* note 49, at 7–9; Kerr & Schneier, *supra* note 49, at 1006.

[250] Bellovin, *supra* note 49, at 16.

[251] *Id.* at 38 n.158.

[252] Mayer, *supra* note 197, at 584.

[253] *Id.*

[254] *See id.* at 583–89 (providing a broad analysis of government malware strategies).

[255] *Id.* at 585.

[256] *Id.* at 586.

[257] *Id.*

[258] Mayer, *supra* note 197, at 586.

[259] *See id.* at 596–608 (discussing metadata and other digital information).

[260] *Id.* at 594.

[261] *Id.*

[262] *Id.*

[263] *Id.* at 641–45 (noting the rationale for always requiring warrants, because of the government's invasion of private spaces).

A different result would arise under the data-centric conception of the Fourth Amendment. This approach emphasizes the protection of *information* rather than devices or spaces.[264] This means that the determining factor of Fourth Amendment protection is the type of information that was seized.[265] In particular, if the information sought is metadata, it receives no Fourth Amendment protection.[266] As Mayer points out, if the government installs 'malware' that reports a suspect's IP address, law enforcement officers can resolve the address to an Internet service provider using a reverse Domain Name System query (which is free and public) and then subpoena the provider to learn the suspect's identity and address.[267] This example illustrates that metadata requires no search warrant because it is not considered a "search" under the Fourth Amendment.[268] By contrast, if the information the government "hacks" is the content of a text message, a warrant is required.[269] Under this data-centric conception, it does not matter if law enforcement "crack[ed] open a closed container" like a smartphone or a computer.[270] If the information is non-content, then no warrant is required.[271] Thus, the government's lawful hacking would be constitutional depending on which avenue of Fourth Amendment interpretation is taken. The following section will explain why this matters by sketching out the policy repercussions of lawful hacking.

3. Policy and Ethical Implications of Fourth Amendment Interpretations

If the government can "lawfully hack" without running afoul of the Fourth Amendment, a number of normative questions arise. This Section will discuss which stakeholders are benefited or harmed under this policy. It will also explain the extent to which the Fourth Amendment succeeds at balancing government investigatory needs with individual privacy in a regime of lawful hacking.

Civil society and civil liberties groups may benefit from a lawful hacking scheme.[272] To reiterate, lawful hacking is presented as an alternative to back doors. A number of civil liberties groups and NGOs submitted amicus briefs to the court in the Apple-FBI dispute.[273] The Electronic Frontier Foundation (EFF) along with 46 technologists, researchers, and cryptographers, wrote a brief

[264] Mayer, *supra* note 197, at 590–93 (discussing the data-centric conception of the Fourth Amendment and its application to various Fourth Amendment doctrines).

[265] *Id.* at 590.

[266] *Id.* at 593.

[267] *Id.* at 596 n.89 (*citing* United States v. Acevedo-Lemus, No. SACR 15-00137-CJC, 2016 WL 4208436, at *3 (C.D. Cal. Aug. 8, 2016)).

[268] *Id.* at 592.

[269] *Id.* at 595.

[270] Mayer, *supra* note 197, at 583.

[271] *Id.* at 593 n.77.

[272] *See generally* Bellovin, *supra* note 49, at 64–65 (arguing that despite ethical qualms inherent in the project, "law enforcement will press for ways to accomplish electronic surveillance").

[273] *See, e.g.*, Brief of Amicus Curiae Electronic Frontier Found. and 46 Technologists, Researchers, and Cryptographers, at 1, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, ED No. CM 16-10 (C.D. Cal. Feb. 19, 2016) (providing an example of an amicus brief submitted in the midst of the Apple-FBI dispute).

arguing that "[e]ncryption and cryptography-based systems . . . are the linchpin of the security of digital devices and the software that runs on them.[274] *Amici* have a vested interest in ensuring that these systems remain both uncompromised and ubiquitous so that everyone can trust that their activities using those devices are secure."[275] On one hand, civil liberties groups and privacy advocates will have achieved their policy aim if lawful hacking is the default policy instead of mandated back doors.[276] The establishment of an alternative to back doors means that the government would not have the power to conduct mass surveillance by exploiting its exceptional access.[277] This is in line with the interests of many civil liberties groups.[278]

On the other hand, a lawful hacking scheme is not a perfect realization of these aims, because government could still access the contents of these private communications.[279] However, under a lawful hacking scheme the government would only be able to access those communications which it can acquire by exploiting existing vulnerabilities.[280] This does not permit the same kind of dragnet surveillance that could occur under a system of mandated back doors.[281] However, the extent of the government's lawful hacking power would depend on whether a warrant was required, as discussed in the previous subsection. If a warrant was not needed, lawful hacking would be subject to little or no judicial oversight.[282] While there may be other policy solutions beyond mandated back doors and lawful hacking, these are the two principal options being considered in the U.S.[283] Overall, the current status quo of lawful hacking is more in line with the interests of civil liberties groups.

Lawful hacking allows the government to work around encryption as much as possible to obtain the information it needs. However, encouraging government to engage in this kind of lawful hacking raises a number of ethical questions. The most pressing ethical question raised by a system of lawful hacking relates to the responsibilities of third parties. The government frequently contracts with private sector companies to carry out components of

[274] *Id.* at 2.

[275] *Id.*

[276] For the positions of several civil liberties and privacy organizations, see amicus briefs before the court in the Apple-FBI dispute. Corrected Brief of Amicus Curiae Electronic Privacy Information Center and Eight Consumer Privacy Organizations, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, ED No. CM 16-10 (C.D. Cal. Feb. 19, 2016).

[277] *See* Haynes, *supra* note 57 (noting the impressive access to personal information that backdoors would present).

[278] *See, e.g.*, Brief of Amicus Curiae Electronic Frontier Found. and 46 Technologists, Researchers, and Cryptographers, at 24, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, ED No. CM 16-10 (C.D. Cal. Feb. 19, 2016) (arguing that there must be limits to the duties that federal courts can impose on third parties).

[279] *See generally* Mayer, *supra* note 197, at 596 n.89 (2018) (*citing* United States v. Acevedo-Lemus, No. SACR 15-00137-CJC, 2016 WL 4208436, at *3 (C.D. Cal. Aug. 8, 2016)) (describing ways that law enforcement officers could use non-content information to obtain content-based information).

[280] *See id.* at 601 (explaining that courts consider exploiting these vulnerabilities as "the online equivalent of a stop-and-identify").

[281] *See* Bellovin, *supra* note 49, at 64 (arguing that merely using existing vulnerabilities would not present the threat of automated abuse against "*everyone*").

[282] *See id.* at 48 (arguing for judicial and technical oversight of lawful hacking, by analogizing the practice to executing a search warrant).

[283] *See generally id.* (analyzing and comparing the policies of mandatory back doors and lawful hacking).

its technical practice. In a regime of lawful hacking, there may be ethical issues with the government hiring private companies to hack other private companies, or assist the government in finding encryption workarounds. One key consideration is whether the government's contractor has a business incentive to assist the government by hacking a competitor. In other words, this lawful hacking scheme might involve the government conscripting companies to undermine the security of their competitors' products. This kind of system would need to be delicately handled to prevent anti-competitive behavior.

A second ethical issue in the lawful hacking regime involves the government's duty to inform companies of vulnerabilities it exploited or intends to exploit. In particular, if a new software update includes a vulnerability that the government can exploit for investigatory purposes, the government would be dis-incentivized to inform the private company. Particularly if national security interests are at stake, the issue of disclosing the vulnerability to the company could even have major repercussions. Clearing information for disclosure and de-classification is often complex, and this kind of system would require careful consideration of when to de-classify and alert a company to its own technical vulnerability. Overall, this dynamic creates conflicting incentives, potentially encouraging the government and the private sector to work against each other.

The question of who benefits from this system of incentives is equally complicated. On one hand, pitting the government's penetration capability against the private sector's security systems could produce more secure systems.[284] It creates an added incentive for private sector companies to keep their systems secure.[285] It is better for the U.S. government to discover a vulnerability than a malicious hacker or a foreign actor.[286] On the other hand, if it *does* end up creating a more secure private sector, the government will ultimately be less and less able to exploit vulnerabilities.[287] This means that the government will have increasingly less access to the information it needs for investigatory purposes.[288] This could indicate that the pendulum would swing back to the U.S. needing legislatively-mandated back doors in the future. Accordingly, the system of lawful hacking relies on the government maintaining a baseline capability to exploit vulnerabilities in company software.

Each Fourth Amendment interpretation also carries its own policy implications. As discussed in the previous subsection, the Fourth Amendment can either be seen as protecting the integrity of *devices* or *information*.[289] Each

[284] *See generally* Cook, *supra* note 11 (noting the security need for encrypting their devices and opposing the U.S. government's attempts to access information in those devices).

[285] *See generally id.* (reaffirming Apple's dedication to keeping its systems secure, even from the U.S. government).

[286] *See* Bellovin, *supra* note 49, at 64 (discussing the possibilities of foreign actors trying to take advantage of vulnerabilities in U.S. systems).

[287] Cook, *supra* note 11.

[288] *See* Bellovin, *supra* note 49, at 64–65 (discussing the consequences to security and law enforcement of hardened communications technologies).

[289] *See* Mayer, *supra* note 197, at 620–21 (noting there is a third option: seeing the two approaches as cumulative and overlapping). However, it is unclear how this would work in cases where the approaches may contradict each other.

avenue has different policy implications. For example, a key component of the data-centric conception is that it creates a distinction between content and non-content.[290] If a data-centric conception were adopted, only government investigation of the content of communications would require a warrant.[291] Non-content (or metadata) would not require a warrant and the government could access it without judicial oversight.[292] As discussed earlier, the distinction between content and non-content is continually dissolving. One important policy implication of this is that most Internet of Things devices would not fall into the Fourth Amendment's purview.[293] Since the data collected and stored by these devices could be more readily defined as metadata, the government may not need a warrant to "lawfully hack" stored Internet of Things information.[294] This would mean that individual health data, collected by Fitbits for instance, would not receive the privacy protection of the Fourth Amendment.[295] This is an entire industry that the government would have wide latitude to search without judicial oversight.[296]

On the other hand, if we adopt the device-centric understanding of the Fourth Amendment, the opposite result might occur. The government would have to obtain a warrant for almost any kind of computer or smartphone penetration.[297] If we understand the Fourth Amendment to protect the integrity of devices as it does physical spaces, then the Fourth Amendment's purview is much larger.[298] The question then would be whether the government's investigatory interests are overburdened. The answer to this question is probably no. Obtaining a warrant from a judge is a relatively routine law enforcement procedure.[299] As a result, it probably does not add a large burden to the investigatory process. The law enforcement officer would only have to show probable cause, or reasonable grounds to believe that a crime is being committed.[300] By the time an investigator has singled out a targeted device for search, they usually have enough factual basis to substantiate probable cause.[301] As a result, a universal warrant requirement for device searches would not impose too high a hurdle for law enforcement. Moreover, "imposing an across-the-board warrant requirement for government malware avoids a foreseeable doctrinal morass about when, exactly, the Fourth Amendment kicks in."[302]

[290] *See id.* at 590–94 (describing the data-centric approach).

[291] *See id.* at 590 (noting the approach of lower courts regarding these issues).

[292] *Id.* at 587.

[293] *Id.*

[294] *See* Bellovin, *supra* note 49, at 13 (noting that metadata is not subject to the warrant requirement of the Fourth Amendment).

[295] Mayer, *supra* note 197, at 595 (explaining that government malware that only reports metadata is not constitutionally regulated).

[296] *Id.*

[297] *See id.* at 638–39 (explaining current and future warrant requirements).

[298] *Id.*

[299] *See generally id.* at 580–82 (describing the text and history of the Fourth Amendment's warrant requirement and how it has been regularized).

[300] *Id.* at 626.

[301] Mayer, *supra* note 197, at 613 (citing Paul Ohm, *Probably Probable Cause*, 94 MINN. L. REV. 1514, 1538–42 (2010)) (arguing that probable cause develops early in online investigations).

[302] *Id.*

Accordingly, a universal warrant requirement makes the legal interpretation of the Fourth Amendment much clearer.

These ethical and policy considerations illustrate the importance of Fourth Amendment jurisprudence for encryption and lawful hacking. As explained above, there are a number of open questions that would arise in a lawful hacking regime where government must work around the absence of back doors. More broadly, looking at encryption policy through this prism of government power reveals repercussions that would not arise under the First Amendment approach described in Part I.A.[303] Examining both approaches allows lawyers, judges and legislators to compare the pros and cons of each avenue. Beyond the established practice of lawful hacking, the U.S. currently has no official legal approach to encryption.[304] Examining the benefits and harms to stakeholders under each approach is a valuable way to begin settling encryption's role in the U.S.

However, an analysis of encryption back doors under U.S. law alone is inherently limited.[305] Encryption is a cross-border phenomenon and many countries are currently dealing with policy dilemmas similar to the ones described here.[306] As a result, an informed legal approach to encryption should consider all available alternatives. Examining encryption under U.K. law is helpful because it presents the opposite legal approach to the U.S.[307] As discussed earlier, encryption also poses international problems which relate to global internet regulation.[308] As a result, a fuller understanding of the international variety in legal approaches to encryption is necessary for sound policy.

The following section will explain the law and policy of encryption in the U.K. Part II.A. will explain the legislative underpinnings of encryption, showing that it mandates back doors on a case-by-case basis. Part II.B. will evaluate this legislation under the U.K.'s "proportionality review" which examines whether a government action was necessary and proportional to the public interest. This comparative analysis is important because it allows stakeholders in both countries to evaluate the effectiveness of particular policies. The U.S. and U.K. can serve as helpful reference points for each other, serving as testing grounds for alternative approaches towards encryption.

[303] *Supra* Part I.A.

[304] *See generally* Mayer, *supra* note 197, at 647 (explaining the concerns that law enforcement agencies have expressed regarding device and communications encryption, to the U.S. Congress).

[305] *See, e.g.*, Haynes, *supra* note 57 (providing an example of debates regarding encryption and mandatory backdoors in the U.K.).

[306] *See, e.g.*, *id*. (noting the contingent political forces at play in the U.K., regarding debates over encryption and mandatory back doors).

[307] *See* DEEKS, *supra* note 23 (noting the U.K.'s necessary and proportionate standard, regarding mandatory backdoors).

[308] *See, e.g.*, Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme, 145 F. Supp. 2d 1168, 1171 (N.D. Cal. 2001) (providing an example of how conflicting legal regimes can potentially aggravate the differences in the ways those states approach legal issues, meant to be covered by treaty, rather than producing cooperation).

IV. PART II: ENCRYPTION UNDER U.K. LAW

In the U.K., encryption is governed by the Investigatory Powers Act (IPA) which has been revised and challenged multiple times since its first incarnation in 2000.[309] Broadly, the IPA regulates the use and oversight of investigatory powers by U.K. law enforcement.[310] This is an important distinction between the U.S. and U.K.'s legal approaches: unlike the U.K., the U.S. has not passed any laws explicitly regulating encryption.[311] While encryption can be situated in existing constitutional literature, the U.S. approach remains unsettled.[312] The lack of legislation on encryption is a policy decision in itself because it maintains the dialectical relationship between the U.S. government's investigatory interest and the private sector's use of strong encryption.[313] This results in the U.S. government's reliance on lawful hacking and encryption workarounds to obtain encrypted communications.[314] Thus, the U.S. government and private sector deal with each case individually, instead of following a uniform policy on encryption.

In this sense, the U.K. has an opposite approach to encryption because the government has explicit power to require back doors if necessary.[315] While the IPA does regulate encryption, its practical impact remains ambiguous in ways that will be explained below. Comparing the U.S. and U.K. approaches brings the policy impacts of back doors into sharp relief. The following section will situate encryption within the U.K.'s legal system and explain the normative considerations that would change the legal analysis. It will also show the policy impact of particular legal interpretations and explain which stakeholders would be affected.

More generally, the encryption debate highlights the challenges of regulating technology. The cross-border nature of the debate teaches important lessons about the value of uniform legal approaches. It also elucidates the opposing interests between the relevant stakeholders: technology companies, government, civil society, and the international community. The norms set by this regulatory debate will influence the regulation of future technologies worldwide.

[309] Regulation of Investigatory Powers Act 2000. c. 23 (Eng).

[310] *Id.*

[311] *See generally* Mayer, *supra* note 197, at 648 (providing an example of the concern that law enforcement agencies have, regarding the lack of Congressional action vis-a-vis encryption).

[312] *See id.* at 640 ("[T]he applicability of super-warrant doctrine to government hacking remains entirely unsettled.").

[313] *See* Bellovin, *supra* note 49, at 64–65 (spelling out the contours of the dialectical relationship between the U.S. government's investigatory interest and moves by the private sector to strengthen encryption of devices).

[314] *See id.* at 30–31 (describing trends inherent in the U.S. technological private sector and law make reliance on "lawful hacking" an unavoidable feature in searching encrypted communications).

[315] Samuel Gibbs, *EU Seeks to Outlaw Backdoors in New Data Privacy Proposals*, The GUARDIAN (June 19, 2017), https://www.theguardian.com/technology/2017/jun/19/eu-outlaw-backdoors-new-data-privacy-proposals-uk-government-encrypted-communications-whatsapp.

A. Encryption Under the IPA: Technical Capability Notices

Under the IPA and its older incarnation, the Regulation of Investigatory Powers Act 2000 (RIPA), a telecommunications operator can be served a "technical capability notice" (TCN).[316] This Section will explain the basic functions of a TCN in order to evaluate its legality and policy impact. The TCN requires an operator to install permanent interception capabilities should the government issue a warrant for particular communications.[317] In other words, the TCN is a confidential way for the government to require a company to maintain access to communications in case the government requests them.[318] Under such notices, the Secretary of State may compel an operator to decrypt intercepted communications.[319] "Amongst other factors, the Secretary of State must further take into account the technical feasibility and likely costs of the request. Should the Judicial Commissioner refuse to approve the notice, the Secretary of State may appeal to the IP Commissioner so as to approve the notice nonetheless."[320] Most importantly, the issuance of such a notice is subject to a necessity and proportionality test, which would be conducted by a Judicial Commissioner.[321] This means that the government objective must be deemed legitimate, and the measures to realize that objective must be deemed necessary.[322] The proportionality analysis of TCNs will be discussed later in this Section.

The process for serving a TCN has several steps.[323] First, the government would issue an interception warrant, which could require a company to turn over requested communications.[324] If a company uses encryption and does have a key, it could assist the government by using the key to decrypt any intercepted messages.[325] If the company or telecommunications operator does not have a key because it uses end-to-end encryption, then all it could do is turn over the encrypted communications.[326] This would be of limited utility to the government investigators since the information would be unintelligible.[327] However, if the operator was served with a TCN, it may be required to install a permanent interception capability.[328] In other words, this would be one way for the government to compel a private corporation to remove any electronic protection like encryption and retain exceptional access.[329] This regulation of

[316] Smith, *supra* note 48.

[317] Regulation of Investigatory Powers Act 2000, c. 23 (Eng.).

[318] *Id.*

[319] Lubin, *supra* note 54.

[320] *Id.*

[321] *Id.*

[322] *See id.* (explaining generally the necessity and proportionality test).

[323] Regulation of Investigatory Powers Act 2000, c. 23 (Eng.).

[324] *The RIP Act*, THE GUARDIAN (Oct. 24, 2000), https://www.theguardian.com/world/2000/oct/24/qanda.

[325] *Id.*

[326] *Id.*

[327] *See What is End-To-End Encryption and How Does it Work?*, PROTONMAIL (Mar. 7, 2018), https://protonmail.com/blog/what-is-end-to-end-encryption (describing that end-to-end encryption prevents people from reading private communications).

[328] Draft Investigatory Powers (Technical Capability) Regulations 2017, SI 2017, pt.1, section 8 (Eng.).

[329] *Id.*

encryption thus came about subtly, as part of a larger and more complex investigatory powers bill.[330] While the word "encryption" is hardly mentioned in the Technical Capability Regulations or the Investigatory Powers Act, the legislation does, as this demonstrates, empower the government to regulate encryption, with the TCN as its main vehicle.[331]

Since the enforcement and application of TCNs remains unclear, there are some open questions on how they will be applied to encryption. For instance, the TCN only requires removal of electronic protection applied "by or on behalf" of the telecommunications operator.[332] Thus, the question of whether an operator would have to remove encryption turns on whether the *user* or the telecommunications operator applies the encryption.[333] In other words, if the user downloads encryption software and applies it to the telecommunication operator's system, then a TCN cannot require the telecommunications operator to remove it.[334] This means that a lot could turn on whether the encryption is regarded as being applied by or on behalf of the operator.[335]

Another ambiguous portion of the regulation involves the practicability of the TCN's request.[336] Both RIPA and the new IPA state that a telecommunications operator can only be required to do what is "reasonably practicable" in response to a warrant or TCN.[337] If a telecommunications operator uses end-to-end encryption, it would be nearly impossible—or at least extremely difficult—to decrypt a communication.[338] A Secretary of State issuing the TCN is required to take into account the technical feasibility.[339] On the one hand, it is not feasible for an operator who provides its users with strong encryption to "decrypt" already existing communications.[340] Thus, a TCN would have to be forward-looking, requiring operators to maintain exceptional access for all future encrypted communications.[341] In other words, a TCN could theoretically be used to require changes in a private company's encryption

[330] Andrew Griffin, *Investigatory Powers Bill Will Not Ban Encrypted Messages Like WhatsApp, But Spies Still Have Access to Much of Communications Data*, THE INDEPENDENT (Nov. 4, 2015), https://www.independent.co.uk/life-style/gadgets-and-tech/news/investigatory-powers-bill-unlikely-to-ban-encrypted-messages-like-whatsapp-but-spies-still-have-a6720811.html.

[331] *See* Draft Investigatory Powers (Technical Capability) Regulations (2017) (this draft was submitted to Parliament under Section 267(3)(i) of the Investigatory Powers Act of 2016 for approval by each House of Parliament).

[332] Regulation of Investigatory Powers Act 2000, c. 23 (Eng.).

[333] *Id.*

[334] *Id.*

[335] *Id.*

[336] *See generally id*, (showing that the Act itself does not speak about the practicability of the TCN's request).

[337] Regulation of Investigatory Powers Act 2000, c. 23 (Eng.).

[338] Andy Greenberg, *Hacker Lexicon: What is End-To-End Encryption?*, WIRED: SEC. (Nov. 25, 2014, 9:00 AM), https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption (explaining the difficulties of decrypting end-to-end encryption).

[339] Graham Smith, *Squaring the Circle of End to End Encryption*, CYBERLEAGLE (May 29, 2017) [hereinafter Smith II], http://www.cyberleagle.com/2017/05/squaring-circle-of-end-to-end-encryption.html.

[340] As explained earlier in this Article, if end-to-end encryption is already in place, the telecommunications operator does not have access to an encryption key. This essentially means that encrypted communications cannot be decrypted upon the government's request.

[341] Smith II, *supra* note 339.

model.[342] In order to comply with a TCN, operators would need to stop offering strong end-to-end encryption.[343] For many operators, the use of encryption is an important part of their platform.[344] This could be problematic if its removal amounts to changing an operator's service or product.[345]

Finally, another important feature of the TCN is its review and appeals process.[346] The bureaucratic review process is important because it determines the extent of the government's power over encryption and civil society's engagement.[347] Under the IPA, the subject of a TCN can request review by the Secretary of State.[348] The Secretary of State then consults the Technical Advisory Board and Judicial Commissioner, who take into account the technical and financial consequences of the TCN.[349] The Commissioner then determines whether the notice is proportionate. Ultimately, the decision of whether to revoke or confirm the TCN rests with the Secretary of State.[350]

Privacy International critiqued the review process on grounds that it does not allow subjects to challenge the TCN before an independent authority like a judge.[351] The review process is currently undertaken only by the Secretary of State with approval by the Investigatory Powers Commission.[352] Additionally, TCNs are legally required to be kept secret.[353] This means that controversial interpretations of TCNs or the IPA more broadly could not be challenged by members of the public.[354] One possibility is that the new Investigatory Powers Commissioner may proactively seek out controversial interpretations of the legislation and make them public.[355]

Understanding the basic functions of a TCN is necessary in order to evaluate its legality and policy impact. Since encryption is a frequently politicized issue where privacy and security are treated as opposing values, a nuanced proportionality analysis of the TCN mechanism can lead to a de-politicized evaluation of encryption policy.[356] The following section will

[342] *Id.*

[343] *Id.*

[344] *Id.*

[345] *Id.*

[346] Regulation of Investigatory Powers Act 2000, c. 23 (Eng.) (outlining the appeals process).

[347] *Id.*

[348] Investigatory Powers Act 2016, c. 25, (Eng.).

[349] *Id.*

[350] *Id.*

[351] *See Privacy International's Landmark Challenge Against UK Government Hacking Will Proceed to the Supreme Court*, PRIVACY INT'L (May 18, 2018), https://privacyinternational.org/press-release/2037/privacy-internationals-landmark-challenge-against-uk-government-hacking-will (explaining that the issue before the Supreme Court is the UK's submission that the decisions are not reviewable by the courts).

[352] Investigatory Powers Act 2016, c. 25, (Eng.).

[353] *See* Smith II, *supra* note 339 (showing that a lawyer interviewed stated, "a telecommunications operator is required to keep a TCN secret.").

[354] *See generally id.* (discussing that since TCNs are required to be kept secret, it would be difficult to challenge them).

[355] *Id.* (illustrating the opinion of the attorney interviewed in this piece. But he also points to a report by the Intelligence Services Commissioner, Sir Mark Waller, discussing that there is precedence for this and that David Anderson QC supported it).

[356] *See generally* Louisa, *The Politics of Encryption*, DVELP (Jan. 17, 2017), https://dvelp.co.uk/articles/politics-of-encryption (generally discussing the effects of encryption of political debates).

introduce the concept of proportionality and explain its role in balancing the competing values at the heart of the encryption debate.

B. Proportionality

Under U.K. law, the IPA must be implemented according to principles of necessity and proportionality.[357] Under the IPA, the Judicial Commissioner must review the Secretary of State's conclusions as to the necessity and proportionality of the TCN.[358] Accordingly, the proportionality determination is important for the enforcement of a TCN.[359] Broadly, the principle of proportionality holds that a government should use means that are necessary and suitable to carry out a legitimate, important aim.[360] At its core, proportionality seeks to balance competing interests and ensure that government actions are narrowly tailored to particular goals.[361] As German administrative law scholar Fritz Fleiner phrased it, proportionality means that "the police should not shoot at sparrows with cannons."[362] More colorfully, proportionality analysis asks whether a proverbial "sledgehammer" was used to crack a nut when "a nutcracker would have sufficed."[363] In the U.K. and in many other countries, proportionality inquiry involves a multi-factor test.[364] Chiefly, the two prongs of "suitability" and "necessity" are the most important parts of the analysis.[365] Suitability asks whether the government objective is rationally connected to the ends sought.[366] Necessity asks whether the right is limited any more than is necessary to accomplish the government objective.[367] Overall, the proportionality analysis has been applied with different levels of "intensity."[368] Much depends on how the terms are defined and how the analysis is framed.[369] The normative understanding and the policy trade-offs of a given government action factor into the ultimate calibration of whether an action is proportional.[370] The following analysis will explain how different understandings of the repercussions of encryption policy would impact the proportionality analysis.

[357] Lorna Cropper, *The Investigatory Powers Act 2016—A "Snooper's Charter" or a Legitimate Surveillance Tool for Today's Society?*, FIELD FISHER (Apr. 2, 2017), https://privacylawblog.fieldfisher.com/2017/the-investigatory-powers-act-2016-a-snoopers-charter-or-a-legitimate-surveillance-tool-for-todays-society.

[358] *Id.*

[359] *See id.* (describing the proportionality analysis).

[360] Jud Mathews, *Proportionality Reviews in Administrative Law*, *in* COMPARATIVE ADMINISTRATION LAW 4 (2017).

[361] *Id.*

[362] *Id.*

[363] Rebecca Williams, *Structuring Substantive Review*, 1 PUB. L. 99, 123 (2016).

[364] *Id.*

[365] *Id.*

[366] *Id.*

[367] *Id.*

[368] *Id.*

[369] Williams, *supra* note 363.

[370] *Id.*

1. *Importance & Legitimacy*

The first step in proportionality review is an evaluation of the importance and legitimacy of the government objective.[371] Rather than being a part of the substantive analysis, these are factors frequently considered to be precursors.[372] They are threshold questions asking whether the government's stated objective in carrying out its policy was sufficiently important and legitimate.[373] In this case, the U.K. government's articulated aim in implementing technical capability notices under the IPA is national security.[374] "Importance" and "legitimacy" are low legal bars, and the technical capability notices probably qualify as advancing an important and legitimate government aim.[375] Additionally, the government traditionally receives broad leeway to advance national security interests.[376] In this case, the government's articulated objective of ensuring national security is probably sufficiently important and legitimate for these prongs of the analysis.[377] The subsequent suitability analysis is a bit more searching, but still a relatively low bar for the government to meet.[378]

2. *Suitability*

The suitability prong of the proportionality analysis asks whether the objective is rationally connected to the ends the decision maker claims it is seeking to achieve.[379] While more probing than the precursory analysis of importance and legitimacy, it is still difficult to make a successful claim on the basis of unsuitability.[380] As Rebecca Williams notes, as long as there is some overlap in the Venn diagram of the rule and the objective, it does not matter that there may be large areas outside the overlap.[381] "Only cases where there is no overlap at all will fail the test."[382] Given the low bar, there is most likely some

[371] *Id.*

[372] *Id.*

[373] *Id.*

[374] *See* A. Michael Froomkin, *Lessons Learned Too Well: Anonymity in a Time of Surveillance*, 59 ARIZ. L. REV. 95, 124 ("Where in the first wave of regulation the main location of regulation . . . regards issues considered to involve crime or public order or to impact national security.").

[375] Williams, *supra* note 363; *see also* Natasha Lomas, *Could the UK be About to Break End-to-End Encryption?*, TECHCRUNCH (2019), https://techcrunch.com/2017/05/27/could-the-uk-be-about-to-break-end-to-end-encryption (noting that the legislation on encryption is an attempt to root out terrorist attacks, suggesting that both the public and the government would find the legislation important and legitimate).

[376] *See* Lizzie Dearden, *One in Four Londoners 'Have Witnessed Extremism,' Poll Suggests*, THE INDEPENDENT (Feb. 2, 2019), https://www.independent.co.uk/news/uk/home-news/terror-attacks-uk-extremism-isis-farright-london-witness-sadiq-khan-a8759216.html (criticizing the national government for failing to adequately protect the public and pushing for more security); Robert M. Chesney, *National Security Fact Deference*, 95 VA. L. REV. 1361, 1362–63 (2009) (explaining that American courts defer to judgments made by the executive branch on matters of national security).

[377] Dearden, *supra* note 376.

[378] Williams, *supra* note 363.

[379] *Id.*

[380] *Id.*

[381] *Id.*

[382] *Id.*

overlap between the TCNs and the government's national security interest.[383] Enabling access to encrypted communications is a measure that is at least rationally related to the public safety aims of preventing criminal activity that is planned or discussed on encrypted communication platforms.[384] Even if criminal activity is only planned or discussed in a minority of encrypted communications, the TCN would likely still qualify as "suitable" under this prong of the analysis.[385]

3. *Necessity*

The necessity prong evaluates whether the fundamental right was limited any more than necessary to accomplish the government objective.[386] In *Bank Mellat*, Lord Sumption cited the necessity test as being "whether a less intrusive measure could have been used."[387] The intrusiveness of the IPA's technical capability notices depends on how a number of ambiguities are resolved.[388] On its face, the IPA seems to require that operators remove end-to-end encryption.[389] If the notices are in fact enforced in this manner, the government wields considerably broader powers under the IPA.[390]

Since the use of end-to-end encryption is a cornerstone of many communications platforms,[391] requiring its removal could be tantamount to changing a company's product. As mentioned earlier in this Article, the introduction of back doors makes communications more vulnerable to hackers.[392] If a company needs to weaken its cybersecurity systems in order to comply with a TCN, it would assume a high financial and litigation risk.[393] Requiring companies to maintain exceptional access would also put private individual communications at risk of being compromised.[394] The potential for infringement on individual privacy also factors into the proportionality

[383] *See* Cropper, *supra* note 357 (explaining that since a "TCN will impose on communication service providers certain obligations which the provider must comply with," it is naturally a related element to the government's national security goal).

[384] *See* Nicholas Watt, Rowena Mason & Ian Traynor, *David Cameron Pledges Anti-Terror Law for Internet After Paris*, THE GUARDIAN (Jan. 12, 2015), https://www.theguardian.com/uk-news/2015/jan/12/david-cameron-pledges-anti-terror-law-internet-paris-attacks-nick-clegg (describing proposed legislation that would allow intelligence agencies to access encrypted communications of terror suspects).

[385] *See* Williams, *supra* note 363 (finding the test of suitability to be whether there is something covered by both the rule and the objective, no matter how much is outside the overlap).

[386] *Id.*

[387] *Id.* at 105 (*citing* Bank Mellat v. Her Majesty's Treasury (No. 2) [2013] UKSC 39 at [20]).

[388] *See* Danny O'Brien & Eva Galperin, *UK's Investigatory Powers Bill: Loopholes Within Loopholes Will Lead to Unbridled Surveillance*, ELEC. FRONTIER FOUND. (Feb. 2, 2016), https://www.eff.org/deeplinks/2016/02/ipb-loopholes-within-loopholes ("[O]ur analysis revealed multiple ambiguities . . . .").

[389] *See* Lubin, *supra* note 54 (stating the IPA allows the government to compel an operator to decrypt communications).

[390] *Id.*

[391] Haynes, *supra* note 57.

[392] *Supra* Section I.

[393] *See* Mike Morel, *The UK Government Should Protect Encryption Not Threaten It*, OPEN RTS. GRP. (May 16, 2017), https://www.openrightsgroup.org/blog/2017/tcns-encryption ("The current ransomware outbreak shows how software vulnerabilities used by security agencies can fall into the wrong hands. There is no reason to think backdoors intentionally created for Government access could not be exploited as well.").

[394] Abelson et al., *supra* note 4, at 70.

analysis.[395] Since TCNs are secret,[396] it is unclear how these kinds of considerations will be navigated and how strict TCN requirements should be. These policy considerations illustrate that a TCN can be an intrusive measure depending on how it is enforced.[397] The question then is whether the government's national security objective can be achieved with a less intrusive measure.

For this part of the inquiry, it is important to note that the use of encryption technology does not render the government powerless in its national security investigations.[398] Law enforcement agencies can still acquire the text of encrypted communications without using back doors.[399] Orin Kerr & Bruce Schneier point out the existence of a number of encryption workarounds, which enable law enforcement to access relevant communications without imposing back doors.[400] Sometimes referred to as lawful hacking, the government can exploit existing software vulnerabilities in order to access encrypted communications.[401] For instance, if the encrypted communications were uploaded to the Cloud and not encrypted, this backed up version could be lawfully accessed by the government.[402] In addition, Kerr and Schneier discuss a number of workarounds including finding or guessing the encryption key.[403] Overall, law enforcement could locate plaintext versions of encrypted communications in many, but possibly not all, cases.[404] The fact that the U.S. government has used these encryption workarounds without relying on mandated back doors is preliminary evidence that a less intrusive solution exists.[405] Indeed, in the past the U.S. has implemented types of exceptional access which it has since discarded.[406] The effectiveness of the alternative methods should be balanced against the consequences of implementing back doors.[407] However, the existence of alternative, less intrusive methods to

[395] Morel, *supra* note 393.

[396] Smith II, *supra* note 339.

[397] *See* Stewart Mitchell, *Gagging Orders: The Internet Surveillance Nobody Can Talk About*, ALPHR (Feb. 9, 2018), https://www.alphr.com/politics/1008443/gagging-orders-internet-surveillance-snoopers-charter ("According to critics of the IP Act, the vague way it has been implemented paves the way for security services to introduce ever more intrusive technologies that companies are unable to contest.").

[398] Kerr & Schneier, *supra* note 49, at 992.

[399] *Id.*

[400] *Id.*

[401] Bellovin, *supra* note 49, at 24–25.

[402] *See id.* at 14–15 (describing how few cloud communications use encryption, creating few problems for law enforcement wire-taps).

[403] Kerr & Schneier, *supra* note 49, at 1007.

[404] *Id.* at 1007–08.

[405] *Id.*

[406] *See, e.g.*, Stephen Levy, *Battle of the Clipper Chip*, N.Y. TIMES (June 12, 1994), http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html?pagewanted=all (describing the downfall of the Clipper Chip after AT&T Bell Laboratories found the technology flawed).

[407] *See* Stepanovich & Karanicolas, *supra* note 67 ("Even if it were possible to build a backdoor which only 'good guys' could use, this would still leave tech companies in the position of having to determine who counts as a 'good guy.'"); Kerr & Schneier, *supra* note 49, at 1007–08, 1019 (discussing that alternative methods include password guessing and accessing plaintext versions, but overall workaround methods are new and still being assessed).

achieve the government's national security aims is *prima facie* evidence that the TCN requirement of the IPA could fail the necessity prong.[408]

Another key consideration in determining the necessity of TCNs is their extra-territorial application.[409] Under the IPA, a telecommunications operator need not be based in the U.K. in order to be served with a TCN.[410] "A technical capability notice may be given to persons outside the United Kingdom (and may require things to be done, or not to be done, outside the United Kingdom)."[411] While broad leeway is typically given to the government in pursuit of national security objectives,[412] this Article argues that such extra-territorial reach is less likely to be necessary under this prong of the proportionality analysis. It would stretch the definition of necessity to say that the U.K. government needs to exercise jurisdiction over non-U.K. operators in order to aptly investigate a future, non-imminent threat.[413] Some geographic limitation of jurisdiction would make TCNs less intrusive.[414] In particular, if TCNs are ultimately used as ways to enforce an encryption ban, their extra-territorial application would mean that the U.K. government effectively becomes an arbiter of how multi-national telecommunications operators design their products.[415]

Since proportionality review is a balancing test, no one factor is dispositive.[416] The analysis involves balancing these normative considerations and deciding how to weigh each one.[417] There are a number of factors weighing against the proportionality of TCN-mandated back doors.[418] The fact that TCNs are secret means any controversial legal interpretations are insulated from public critique.[419] This makes it difficult to judge whether the actual enforcement of TCNs will meet requirements of necessity and proportionality.[420] Nevertheless, the negative externalities of adopting back doors would weigh against finding

[408] *See* Stepanovich & Karanicolas, *supra* note 67 (finding alternative methods available to law enforcement).

[409] *See* David S. Kris, *Trends and Predictions in Foreign Intelligence Surveillance: the FAA and Beyond*, 8 J. NAT'L SECURITY L. & POL'Y, 377, 409 ("In case the UK bill is not clear enough on its face, the Electronic Frontier Foundation (EFF) asserts in public comments on the bill that the "common term for 'equipment interference' is 'hacking': breaking into and *remotely* controlling devices.") (emphasis added).

[410] Investigatory Powers Act 2016, c. 25, § 253(8) (Eng.).

[411] *Id.*

[412] *See* Dearden, *supra* note 376 ("They think the security machine and counter-terrorism policing is where it all happens but the statistics prove that in this country, public support is vital and it is working.").

[413] Williams, *supra* note 363.

[414] A and others v. Secretary of State for the Home Department, [2004] UKHL 56.

[415] *Id.* (holding that detention of terrorist suspects in Belmarsh was disproportionate because national subjects were not so detained and because it was a "three walled prison" where the individuals were free to leave.)

[416] Williams, *supra* note 363.

[417] *Id.*

[418] *See* Anthony Cuthbertson, *Plans for Increased Internet Surveillance Revealed in Leaked Documents*, NEWSWEEK (May 5, 2017, 8:42 A.M.), https://www.newsweek.com/plans-increased-internet-surveillance-revealed-leaked-documents-595139 (describing some of the opposition to TCNs, indicating that there are normative, value judgements to be made about their social utility).

[419] Smith II, *supra* note 339; *see also* Cuthbertson, *supra* note 418 ("'These powers could be directed at companies like WhatsApp to limit their encryption . . . but if the powers are exercised, this will be done in secret,' Jim Killock, executive director of Open Rights Group, said in an emailed statement to Newsweek.").

[420] *See* Williams, *supra* note 363 (discussing necessity and proportionality requirements).

them to be a necessary measure.[421] Back doors make security systems inherently less secure.[422] If exceptional access is retained for government use, malicious actors and foreign states could exploit those built-in vulnerabilities.[423] Businesses in the U.K. would be burdened by the added cost of compliance and increased risk of litigation due to data breaches.[424] Moreover, some telecommunications operators rely on strong encryption as a cornerstone of their service or product.[425] If the removal of strong encryption amounts to changing a particular company's product, requiring back doors would present a considerable burden.[426] Telecommunications operators that handle individual communications also risk compromising the privacy of that information if back doors are implemented.[427] Given the existence of alternative options like encryption workarounds described above, these are strong considerations weighing against the necessity of back doors.

However, the result of the proportionality analysis would depend on how "intensely" the proportionality test were applied.[428] If the national security interests of the government are given particular weight,[429] a less probing proportionality analysis may be conducted that is more deferential to government needs. Even under a more searching analysis, the understanding of encryption as a security issue as well as a privacy issue may tip the scales against the proportionality of TCN-mandated back doors.[430] The following section will analyze this balancing test more deeply, taking into account some of the normative considerations discussed above.

4. Fair Balance Test

A final, fair-balance test is sometimes included in proportionality analysis.[431] It asks whether there is a fair balance between the rights of the

[421] Danny Palmer, *Backdoors, Encryption and Internet Surveillance: Which Way Now?*, ZDNET (June 15, 2017), https://www.zdnet.com/article/backdoors-encryption-and-internet-surveillance-which-way-now.

[422] Rob Merrick, *UK's Ex-Spy Chief Warns Amber Rudd's Plan to Pass New Smartphone Encryption Law Is Dangerous*, THE INDEPENDENT (July 10, 2017, 12:04 PM), https://www.independent.co.uk/news/uk/politics/uk-ex-spy-chief-amber-rudd-home-secretary-smartphone-encryption-law-dangerous-terrorism-isis-a7833211.html.

[423] *Why The Government Wants A Mandatory 'Backdoor' On Encrypted Technology*, THE WEEK (Sept. 3, 2018), https://www.theweek.co.uk/96224/why-the-government-wants-a-mandatory-backdoor-on-encrypted-technology.

[424] *See id.* (explaining why companies would not like a backdoor to their encryption in their products).

[425] Rob Price, *Whatsapp Reportedly Refused To Build An Encryption Backdoor For The UK Government*, BUS. INSIDER (Sept. 20, 2017, 10:46 AM), https://www.businessinsider.com/whatsapp-refused-encryption-backdoor-uk-government-report-2017-9.

[426] *See id.* (explaining how WhatsApp was built with end-to-end encryption).

[427] Gary Eastwood, *5 Of the Biggest Cybersecurity Risks Surrounding IoT Development*, NETWORK WORLD (June 27, 2017, 11:32 AM), https://www.networkworld.com/article/3204007/internet-of-things/5-of-the-biggest-cybersecurity-risks-surrounding-iot-development.html.

[428] *See Encryption: A Matter of Human Rights*, AMNESTY INT'L (2016), https://www.amnestyusa.org/files/encryption_-_a_matter_of_human_rights_-_pol_40-3682-2016.pdf (explaining the assessment of the proportionality analysis).

[429] *Encrypted Technology*, *supra* note 421.

[430] Rick Smith, *Understanding Encryption and Cryptography Basics*, TECHTARGET (Jan. 2003), https://searchsecurity.techtarget.com/Understanding-encryption-and-cryptography-basics.

[431] Williams *supra* note 363.

individual and the interests of the community in the decisionmaker's action.[432] This part of the analysis would contextualize the government action to evaluate whether it was justified on "compelling grounds of public interest" or involved "issues of social or economic policy."[433] Such considerations would impact the intensity of proportionality review, in that greater deference would be given to the government action in matters of pressing public interest.[434]

The outcome of a "fair balance" test depends on which considerations are placed and weighted on either side of the scale.[435] Encryption is often framed as an issue of compelling public interest, meriting a less intense proportionality analysis.[436] Under this understanding, the scale is conceptualized as a balance between the community's interest in national security and the derogation of relevant rights such as privacy, corporate freedom, and free expression, which might be chilled by increased government access to private communications.[437] However, the framing of "community interests" should better consider the ways in which back doors would negatively affect national security interests.[438]

A number of normative considerations should affect the conceptualization of this fair balancing test.[439] As discussed earlier, the introduction of back doors negatively affects the U.K.'s security because it makes telecommunications operators vulnerable to cyberattacks.[440] If back door keys exist for government access, they can also fall into the hands of foreign actors and hackers.[441] If the contents of those communications are, in fact, of national security interest to the U.K., then their procurement by an adverse entity would be problematic.[442] The existence of back doors also opens the U.K. up to cyberattacks that could lead to physical damage of infrastructure.[443] While the IPA appears narrowed to "telecommunications operators," the platforms affected would touch a variety of industries that handle sensitive information.[444] Making that information less

[432] *Id.*

[433] *Id.* (*citing* Axa Gen. Ins. Ltd v. HM Advocate, [2011] UKSC 46).

[434] *Id.*

[435] *See id.* (explaining the pros and cons of the fair balance test).

[436] Gillian Black & Leslie Stevens, *Enhancing Data Protection and Data Processing in the Public Sector: The Critical Role of Proportionality and the Public Interest*, SCRIPTED (Apr. 14, 2013), https://script-ed.org/article/enhancing-data-protection-data-processing-public-sector-critical-role-proportionality-public-interest.

[437] *See id.* (explaining the balancing interests).

[438] Anja Kaspersan, *Can You Have Both Security and Privacy in the Internet Age?*, WORLD ECON. F. (July 21, 2015), https://www.weforum.org/agenda/2015/07/can-you-have-both-security-and-privacy-in-the-internet-age.

[439] Veena Srirangam, *A Difference in Kind–Proportionality and Wednesbury*, 4 IALS STUDENT L. REV. 1, 44, 59 (2016).

[440] Chris Graham, *NHS Cyber-Attack: Everything You Need to Know About 'Biggest Ransomware' Offensive in History*, THE TELEGRAPH (May 20, 2017, 1:36 AM), https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive.

[441] *See* Price, *supra* note 425 (explaining how companies fear vulnerability to third parties by giving the government backdoor access).

[442] *See* Graham, *supra* note 440 (explaining how hospitals and health services were affected by cyber-attacks).

[443] *Id.*

[444] Investigatory Powers Act, Ch. 25 § (5)(a)(ii) (2016).

secure by introducing back doors would negatively affect U.K. security.[445] As such, the picture of encryption as a balance between privacy and national security is incomplete. There are important national security reasons for refraining from introducing back doors.[446]

In conducting a fair balance test, it is also important to consider the financial impact of back doors on the U.K. economy.[447] If U.K.-based communications platforms are perceived as less secure because they are legally required to maintain back doors, investment will flow out of the U.K. and into countries whose companies do use strong encryption.[448] For example, if a bank or hedge fund is seeking to create a branch operating out of the U.K., the communication platform they use to host their internal messages, consumer data, or financial analysis could be served with a TCN.[449] If they are required to maintain a back door, their data breach risk and potential liability in the event of attack would increase.[450] The ambiguity of the TCN's enforcement also makes companies less likely to set up in the U.K. and investors less likely to invest in companies with a data breach risk.[451] The increased risk and cost of compliance would thus deter businesses from operating in the U.K..[452]

Relatedly, the introduction of back doors would impact the way other countries perceive the trustworthiness of U.K. communications.[453] Peter Swire and Kenesa Ahmad argue that encryption is important for globalization because of the "least trusted country problem."[454] This means that the level of trust placed in "data traveling through the Internet becomes that of the country that we trust least."[455] Since online communications are globally interconnected, the security of one country's communications affects that of others.[456] Not only is the reputation of U.K. communications affected, but the security of the global system is also impacted by the U.K.'s policy on back doors.[457]

[445] Ewen MacAskill, *Major Cyber-Attack an UK a Matter of 'When, Not If' – Security Chief*, THE GUARDIAN (Jan. 23, 2018, 1:56 PM), https://www.theguardian.com/technology/2018/jan/22/cyber-attack-on-uk-matter-of-when-not-if-says-security-chief-ciaran-martin.

[446] Graham, *supra* note 440.

[447] *See* Bell, *supra* note 173 (explaining how backdoors have affected the U.S. economy).

[448] Daniel Eran Dilger, *After Apple's Objections, UK Removes Encryption Backdoors From Investigatory Powers Bill Before Passing*, APPLEINSIDER (June 7, 2016, 2:43 PM), https://appleinsider.com/articles/16/06/07/after-apples-objections-uk-removes-encryption-backdoors-from-investigatory-powers-bill-before-passing-.

[449] Paul Biegler, *Our Digital Dilemma: Does Latest Cybersecurity Legislation Go Too Far?*, SYDNEY MORNING HERALD (Sept. 23, 2013), https://www.smh.com.au/national/our-digital-dilemma-does-latest-cybersecurity-legislation-go-too-far-20180919-p504oh.html.

[450] *Id.*

[451] *See* Dilger, *supra* note 448 (explaining how apple objected to the back door).

[452] Biegler, *supra* note 449.

[453] *See* Juliette Garside, *The Chinese Firm Taking Threats to UK National Security Very Seriously*, THE GUARDIAN (Aug. 7, 2016, 2:00 PM), https://www.theguardian.com/technology/2016/aug/07/china-huwaei-cell-uk-national-security-cyber-surveillance-hacking (explaining how other countries companies are finding the TCN as a threat).

[454] Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416, 419 (2012).

[455] *Id.*

[456] *Id.* at 418.

[457] Biegler, *supra* note 449.

These normative and policy considerations impact the fair balance test and proportionality review more generally.[458] Instead of assuming a binary of national security interests on one side of the scale and privacy rights on the other, there are a number of financial, civil liberties, and security interests supporting strong encryption.[459] Thus, the "public interest" factors may be weighed against compelled back doors.[460] The impact on individual privacy and the burden it would place on U.K. businesses also changes the "intensity" of the proportionality review.[461] If a disproportionate burden would be placed on individuals whose communications would be less secure and telecommunications operators whose businesses would be meaningfully affected, then the public interest considerations of TCNs would need to be quite weighty.[462] Given that there are a number of public interest reasons against compelled decryption, a strong case can be made that they would not be necessary or proportional.[463]

V. CONCLUSION

The extent of encryption's impact depends largely on how it is regulated. The chosen system of governance could change the power dynamic between government and civil society, affect a country's economic wellbeing, protect network security, or introduce vulnerabilities. If strong encryption is uniformly banned, the government will have greater ability to monitor private communications. On the other hand, if the government has no access to encrypted communications, national security investigations may be encumbered. This Article suggests that there are many layers of nuance between these two options.

Returning to the initial inquiry introduced at the outset of this paper, there are a number of legal frameworks that courts and legislators could use to approach encryption. Part I presented the argument that encryption, and all other types of code, should be regulated as "speech" under the First Amendment. Legally, this is problematic because the existing free speech jurisprudence in the U.S. does not account for the variety in types of code.[464] The argument of "code as speech" turns on the idea of its expressiveness. By analogy, the question posed above is whether code is more like a typewriter or the poem written using the typewriter. This Article suggests that not all code is equally expressive, and falls on a spectrum. In other words, some code is more functional like a

[458] Srirangam, *supra* note 439, at 47.

[459] Nicole Perlroth, *Security Experts Oppose Government Access to Encrypted Communication*, N.Y. TIMES (July 7, 2015), https://www.nytimes.com/2015/07/08/technology/code-specialists-oppose-us-and-british-government-access-to-encrypted-communication.html.

[460] Steve Ranger, *Encryption Backdoors Are Against US National Interest, Say Lawmakers*, ZDNET (Dec. 22, 2016, 3:08 PM), https://www.zdnet.com/article/encryption-backdoors-are-against-us-national-interest-say-lawmakers.

[461] Srirangam, *supra* note 439, at 47.

[462] *See* Ranger, *supra* note 460 (explaining how backdoors would affect national interest and what should be considered).

[463] *See id.* (explaining the consequences of the policy requiring back doors).

[464] David Golumbia, *Code Is Not Speech*, UNCOMPUTING (Apr. 13, 2016), https://www.uncomputing.org/?p=1716.

typewriter, while some is more expressive like a poem. Given that its purpose is to obscure rather than communicate information, encryption code is probably more functional than expressive. A First Amendment approach to encryption needs this kind of narrowing principal. Otherwise, if *all* code is considered speech than the government cannot regulate it as easily. As explained in Part I, the First Amendment protects speech from government regulation by requiring the government to show a very compelling public interest before passing a law. Making it more difficult for government to regulate code (and thus, encryption) means that back doors are unlikely to be mandated but it also means also that justifiable regulation of code may not be possible.

The second argument under U.S. law explained above focused on a Fourth Amendment legal theory which suggests that encryption should be regulated as a type of government "search." This theory involves examining the legality of encryption technologies through the prism of government investigatory power. In a country without legally mandated back doors,[465] the government will resort to methods like lawful hacking in order to acquire information necessary for criminal investigations. This Article argues that a universal warrant requirement should be imposed on all instances of lawful hacking. Since the Fourth Amendment acts as a check on government investigatory power and a protection of individual privacy,[466] it should be interpreted to require a warrant for lawful hacking. As a policy matter, the presence of such a warrant requirement adds a valuable protection on individual privacy without burdening law enforcement investigations or muddling Fourth Amendment doctrine.

In the U.K., back doors are regulated through the TCN mechanism authorized by the IPA.[467] These TCNs are used to require individual telecommunications operators to implement back doors at the government's request.[468] Since a TCN must be deemed "necessary and proportional" by a judicial commissioner before being issued,[469] the analysis above examined the extent to which back doors are necessary and proportional under U.K. law. This paper argues that TCNs may fail the "necessity" prong of proportionality review, suggesting that the policy scheme involves government overreach. The intrusiveness of TCNs on the products and services of telecommunications operators paired with the existence of alternative policy avenues suggests that mandated back doors are not truly "necessary" as the law requires.

The analysis of legal approaches to encryption in the U.S. and U.K. is significant because it elucidates the effects of particular policies. The U.K.'s Investigatory Powers Act allows the government to mandate back doors as

[465] Sharon Bradford Franklin, *Looking Down Under for a Back Door*, SLATE (Oct. 5, 2018, 1:21 PM), https://slate.com/technology/2018/10/australia-u-s-encryption-backdoor-law.html.

[466] U.S CONST. amend. IV.

[467] Matt Burgess, *Government Plans To Push Through Powers That Will Force Tech Giants To Hand Over Encrypted Messages*, WIRED (May, 24, 2017), https://www.wired.co.uk/article/uk-government-encryption-snoopers-charter.

[468] Investigatory Powers Act, Ch. 25 § (87)(1)(a) (2016).

[469] Lubin, *supra* note 54.

necessary.[470] The U.S., by contrast, has no legislation mandating back doors,[471] but the government can lawfully hack to access encrypted communications by exploiting existing vulnerabilities.[472] The evaluation above of harms and benefits to stakeholders reinforces the notion that back doors have negative policy consequences. Comparing the U.S. and U.K.'s dispositions towards encryption shows the wide spectrum of possible policies. Comparing these two approaches brings the pros and cons of each option into sharp relief. The nature of encryption policy depends on the legal justifications that sustain it. It has the capacity to destabilize existing dynamics between the private and public sector, and between government and civil society. The regulatory treatment of encryption will determine the extent of its impact.

[470] Investigatory Powers Act, Ch. 25 § (87)(1)(a) (2016).

[471] Franklin, *supra* note 465.

[472] Ben Buchanan, *Bypassing Encryption: 'Lawful Hacking' is the Next Frontier of Law Enforcement Technology*, THE CONVERSATION (Mar. 16, 2017, 8:05 PM), http://theconversation.com/bypassing-encryption-lawful-hacking-is-the-next-frontier-of-law-enforcement-technology-74122.