2016

Guardians of Your Galaxy S7: Encryption Backdoors and the First Amendment

Allen Cook Barr

Note

Guardians of Your Galaxy S7: Encryption Backdoors and the First Amendment

*Allen Cook Barr**

On December 2, 2015, two armed individuals killed fourteen people in San Bernardino, California.[1] In the aftermath of the shooting, investigators began looking into evidence they could obtain from the shooters' electronic devices. However, when they did so, they were met with a roadblock: encryption.[2] Encryption is everywhere, from toasters[3] to televisions.[4] Encryption is the key to privacy in the digital era;[5] it makes secure online banking, trading, and purchasing possible.[6] The use of

* CIPP/US; J.D. Candidate 2017, University of Minnesota Law School; B.A. Physics & Philosophy, Drake University. Thank you to Professor Richard Frase, Anna Luczkow, and Jerome Borden for their feedback, comments, and suggestions. Additional thanks to Professor Christopher Soper and Professor Jennifer McCrickerd for their guidance in developing my writing and analytical skills. Finally, thank you to my friends and family for their support, both as I was writing this Note and throughout my life.

1. Adam Nagourney et al., *San Bernardino Shooting Kills at Least 14; Two Suspects Are Dead*, N.Y. TIMES (Dec. 2, 2015), http://www.nytimes.com/2015/12/03/us/san-bernardino-shooting.html.

2. *See* Pierre Thomas, *Feds Challenged by Encrypted Devices of San Bernardino Attackers*, ABC NEWS (Dec. 9, 2015), http://abcnews.go.com/US/feds-challenged-encrypted-devices-san-bernardino-attackers/story?id=35680875.

3. *Cf.* Chris Orr, *Hacking the Internet of Things: Beware of the Toasters*, TRIPWIRE: THE STATE OF SECURITY (Dec. 23, 2014), http://www.tripwire.com/state-of-security/risk-based-security-for-executives/connecting-security-to-the-business/hacking-the-internet-of-things-beware-of-the-toasters (noting that hackers may soon target appliances such as toasters).

4. *See* Leo Kelion, *Samsung's Smart TVs Fail To Encrypt Voice Commands*, BBC (Feb. 18, 2015), http://www.bbc.com/news/technology-31523497.

5. *See Privacy in the Digital Age: Encryption and Mandatory Access: Hearing Before the Subcomm. on the Constitution, Federalism, and Prop. Rights of the S. Comm. on the Judiciary*, 105th Cong. 4 (1998) [hereinafter *Privacy in the Digital Age*] (statement of Sen. Russell D. Feingold, Member, Subcomm. on the Constitution, Federalism, & Prop. Rights of the S. Comm. on the Judiciary).

6. *1.7 Why Is Cryptography Important?*, EMC^2, http://www.emc.com/emc

encryption, however, comes with law enforcement costs.[7] While encryption may make it impossible for a criminal to hack your bank account, it may also make it impossible for law enforcement to gain access to that criminal's information, even after a court has held that such access is a lawful search and seizure.[8] In response to these issues, law enforcement personnel have sought to push technology companies towards implementing tools that would allow them to bypass encryption when needed as part of an investigation.[9] Technology companies on the other hand, spurred by the Edward Snowden revelations of 2013,[10] have been very reluctant to comply, fearing the backlash of customer reaction they believe would accompany it.[11] Thus, rather than seeking voluntary assistance from software developers, some individuals in law enforcement have begun to push for legislation on so-called "encryption backdoors," tools that would provide for government access to encrypted communications.[12]

The call for encryption backdoors raises a significant First Amendment issue. Originally debated in the mid-to-late 1990s, computer source code is arguably First Amendment protected speech.[13] Indeed, several cases in the 1990s challenged export control restrictions on computer source code as unconstitutional

-plus/rsa-labs/standards-initiatives/why-is-cryptography-important.htm (last visited Oct. 12, 2016).

7. *Privacy in the Digital Age*, *supra* note 5, at 1 (statement of Sen. John Ashcroft, Chairman, Subcomm. on the Constitution, Federalism, and Prop. Rights of the S. Comm. on the Judiciary).

8. Matt Apuzzo et al., *Apple and Other Tech Companies Tangle with U.S. over Data Access*, N.Y. TIMES (Sept. 7, 2015), http://www.nytimes.com/2015/09/08/us/politics/apple-and-other-tech-companies-tangle-with-us-over-access-to-data.html (describing how Apple indicated it could not turn over iMessages even after a court ordered it to do so).

9. *See id.*

10. *Snowden Surveillance Archive*, CANADIAN JOURNALISTS FOR FREE EXPRESSION, https://snowdenarchive.cjfe.org/greenstone/cgi-bin/library.cgi (last visited Oct. 12, 2016).

11. *See* Apuzzo et al., *supra* note 8.

12. *See, e.g.*, J. David Goodman, *New York City Police Commissioner Says Attacks Will Force Changes in Tactics*, N.Y. TIMES (Nov. 15, 2015), http://www.nytimes.com/live/paris-attacks-live-updates/bratton-says-attacks-will-force-law-enforcement-to-change-tactics (quoting the New York City police commissioner as saying encryption access was something that "is going to need to be debated very quickly").

13. *Cf.* Dan L. Burk, *Software as Speech*, 8 SETON HALL CONST. L.J. 683, 691 (1998) (discussing the new problems computer code was creating in the First Amendment context in the 1990s).

prior restraints on free speech.[14] These cases, however, differ from modern proposals, which would compel speech by requiring developers to write in encryption backdoors.[15] Although both courts and commentators have considered whether prior restraints like those challenged in the export control cases are constitutional, relatively little analysis has been performed on when, if ever, compelling software backdoors would satisfy constitutional requirements.

This Note argues that the broad-sweeping encryption backdoor regimes typically suggested by law enforcement personnel would not satisfy the First Amendment's prohibition against compelled speech. Although there may be some legislative or judicial actions the government could take to allow access to some encrypted communications, requiring changes to the source code for all of a company's devices is not a permissible response. Part I of this Note provides the technological background necessary for a basic understanding of how encryption software is written and operates. This Part then reviews Supreme Court precedent on compelled speech, as well as past attempts by the government to regulate or otherwise curtail encryption technologies. Part II examines how current proposals for encryption backdoors implicate compelled speech issues in a way that past attempts to regulate encryption did not. After distinguishing past attempts from compelled backdoors, Part II analyzes the arguments for and against protecting source code, arguing that source code may only be compelled in the presence of a "clear and present danger," and that broad encryption backdoors fail this test. Given that broad backdoors in all devices are impermissible, Part III offers some possible solutions that would enable law enforcement to access encrypted information in narrowly tailored circumstances. Although preliminary, Part III provides two examples of how—for specific individuals—law enforcement could gain access to both communications and (in the right circumstances) stored encrypted information by working with technology companies.

14. *See, e.g.*, Bernstein v. U.S. Dep't of State, 974 F. Supp. 1288 (N.D. Cal. 1997).

15. *See* Apuzzo et al., *supra* note 8.

I. BACKDOOR'S BACKGROUND: TECHNOLOGICAL AND LEGAL ISSUES SURROUNDING ENCRYPTION BACKDOORS

Encryption regulation embraces several distinct areas of inquiry: software development, the mathematical mechanics of encryption, and First Amendment free speech concerns. This Part provides an overview of the technology involved in encryption backdoors as well as how the courts have addressed regulations of speech similar to encryption backdoors in the past.

A. SOFTWARE DEVELOPMENT AND THE MECHANICS OF ENCRYPTION

A natural starting point for understanding the legal issues encryption backdoors implicate is the technology itself. The technological components of encryption can broadly be broken down into two key areas: the process of creating a computer application in general and the mathematical underpinnings that make encryption technologies possible.

1. The Process of Software Development

Broadly speaking, computer programs are sets of instructions that tell the various hardware components of a computer (processor, random-access memory, display, etc.) to perform a particular action.[16] Each action is itself miniscule, such as "set the pixel located at 917, 229 to color code 7C0019."[17] However, the sheer speed with which computers perform individual steps brings these steps together to quickly produce end results.[18] Understanding the process of translating computer steps from an idea in the programmer's mind into instructions interpretable by a computer processor is key to appreciating how encryption backdoors raise First Amendment concerns. Beginning

16. *See* TONY GADDIS, STARTING OUT WITH C++: FROM CONTROL STRUCTURES THROUGH OBJECTS 4–6 (7th ed. 2012).

17. This would still need to be further broken down into more steps, such as determining what amount of red, green, and blue produces color 7C0019. *See* Jeff Tyson, *How LCDs Work*, HOWSTUFFWORKS (July 17, 2000), http://electronics.howstuffworks.com/lcd5.htm.

18. *See, e.g.*, *Intel Core i7-4770K*, PCMAG (June 1, 2013), http://www.pcmag.com/article2/0,2817,2419798,00.asp (reviewing a consumer-grade processor capable of performing thirty-two operations per clock-tick with a clock speed of 3.5 gigahertz). This leads to a total of over one hundred billion operations per second.

with the end result of computer programming—the computer application—and working backwards is helpful in this regard.[19]

When most individuals use a computer for a particular task, they begin by opening the application needed to complete that task. On its surface, an application may appear to be a single file; however, an application is really a collection of two components: machine code (instructions telling the computer what to do), and resources or assets (content provided by the application developer for the application to use, such as menu text and button icons).[20] The machine code included with the application can be interpreted by a computer processor. Machine code, however, is very difficult for a human to read or modify.[21] To aid developers in writing instructions that computers can understand, tools known as compilers have been developed.[22] Compilers enable developers to write code in a way that is meaningful to humans (such as "areaOfRectangle = baseLength * sideHeight") and then have it translated into machine code for execution by the computer.[23] This human readable code, known as "source code," is what developers write in to express their ideas regarding the steps a computer is to perform.[24] Free speech issues come to the forefront at this point. As content that is meaningful to humans, source code is arguably

19. The steps a computer takes when running the application are not particularly relevant to a discussion of how source code should be treated under the First Amendment. For a technical discussion of how instructions are given to computer processors, see generally JOHN L. HENNESSY & DAVID A. PATTERSON, COMPUTER ARCHITECTURE apps. A-1–A-54 (5th ed. 2012).

20. *Glossary*, ANDROID DEVELOPERS, https://developer.android.com/guide/appendix/glossary.html (last visited Oct. 12, 2016).

21. Y. DANIEL LIANG, INTRODUCTION TO JAVA PROGRAMMING 7 (10th ed. 2015). Machine code is literally a string of binary numbers, which are sent as high and low-voltage electrical impulses to a computer's components; those components are then hardwired to respond in a particular way. ERIC WALKINGSHAW, MACHINE CODE AND HOW THE ASSEMBLER WORKS 6, 8 (Mar. 8–13, 2013), http://web.engr.oregonstate.edu/~walkiner/cs271-wi13/slides/11-MachineCode.pdf.

22. LIANG, *supra* note 21, at 8.

23. *Id.* This is still a massive gloss of how compilers operate. The essential point is that compilers convert statements in a language understandable by humans to a language understandable by computers. *Id.* Different programming languages and computer hardware may have more or fewer steps involved in the process of converting human readable code to machine code. *See, e.g.*, *id.* at 16–18 (describing the additional steps Java requires to convert source code into machine code).

24. GADDIS, *supra* note 16, at 11.

speech or expressive conduct,[25] and, therefore, government regulation of it is generally prohibited by the Constitution.[26]

2. AN OVERVIEW OF ENCRYPTION TECHNOLOGY

Fundamentally, there is nothing about computer encryption that could not be accomplished by a human using pencil and paper, given enough time.[27] Indeed, encryption technology dates back to ancient times,[28] and computers have merely allowed increased complexity in encryption methods and the ability of others to intercept and decrypt messages.[29] What was once difficult or impossible to decrypt may become possible with advances in technology.[30] As a matter of fact, only one form of encryption has been shown to be impossible to break, even given infinite time and resources, and its use is generally impracticable for everyday usage.[31] For all other forms of encryption, the question is not whether the encryption can be broken, but how long the decryption process will take.[32]

25. This was the main issue of several cases in the 1990s that considered the legality of the export bans discussed *infra* Part I.B.1. *See, e.g.*, Bernstein v. U.S. Dep't of State, 974 F. Supp. 1288, 1306 (N.D. Cal. 1997) (considering whether export regulation of cryptography suppressed protected expression).

26. U.S. CONST. amend. I ("Congress shall make no law . . . abridging the freedom of speech . . . ."); R.A.V. v. City of St. Paul, 505 U.S. 377, 382 (1992) ("The First Amendment generally prevents government from proscribing speech . . . or even expressive conduct . . . ." (citations omitted)); *see also infra* Part II.B (discussing the application of the First Amendment to source code).

27. *Cf.* RANDALL MUNROE, WHAT IF? 98 (2014) ("[A] human running through computer chip benchmark calculations by hand, using pencil and paper, can carry out the equivalent of one full instruction every minute and a half." (footnote omitted)).

28. Chris Savarese & Brian Hart, *The Caesar Cipher*, TRINITY C., http://www.cs.trincoll.edu/~crypto/historical/caesar.html (last visited Oct. 12, 2016).

29. BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY 8 (1st ed. 1994).

30. *Id.* at 7.

31. *Id.* at 13–14. That one method is a one-time pad. Its operation is fairly simple: given a secret message (in binary form) and a random "pad" of bits as long as the message, an XOR operation is performed on each bit of the message with each bit of the pad. So long as the pad is truly random and is never reused, it cannot be broken. The difficulty in everyday usage is that the two communicating parties must find some way to securely exchange their pads. RUBY B. LEE, SECURITY BASICS FOR COMPUTER ARCHITECTS 31 (Mark D. Hill ed. 2013).

32. *See, e.g.*, *Security and Freedom Through Encryption (SAFE) Act: Hearing on H.R. 695 Before the H. Comm. on the Judiciary*, 105th Cong. 45 (statement of William P. Crowell, Deputy Director, National Security Agency) ("If all the personal computers in the world—260 million computers—were put to work on a single PGP-encrypted message, it would still take an estimated 12

Despite being technically breakable, modern encryption technologies are still very secure. The encryption program, Pretty Good Privacy (PGP), referenced by the Deputy Director of the National Security Agency (NSA) provides an excellent example for explaining how modern encryption software works.[33] PGP is a public-key cryptography system.[34] This means that sending a secret message with it involves the use of two keys: one to encrypt the message (the public key) and a different one to decrypt the message (the private key).[35] Public and private keys can be thought of as keys to a special kind of vault: the public key allows any member of the public to put a message in the vault (preventing anyone else from reading it), however, only the private key holder can open the vault and read all the messages that have been placed inside it.[36] More technically, the keys used for public-key encryption are a pair of very large numbers with particular mathematical properties, such that someone with the private key can easily decrypt messages encrypted with the public key. Deducing the private key from the public key, however, is computationally unfeasible (although not theoretically impossible).[37] Software developers have utilized these properties to write programs that can enable anyone to send messages with strong encryption.[38] As a result, public key encryption software is now widely available to the consumer public, provided that people know how to use it. Similar tools are also available for encrypting information outside of the person-to-person communication context and are used in a variety of applications, including inter alia wireless passwords, banking access, and computer file systems.[39]

million times the age of the universe, on average, to break a single message . . . .").

33. Obviously, the particular encryption scheme used will vary from situation to situation. Public-key encryption is useful for communications, but is unnecessary for data storage, such as information that is kept on a phone or computer, but never transmitted. Nevertheless, this public-key encryption example highlights the issues germane to the most common situation in which encryption problems arise: communications between criminals.

34. PGP CORP., AN INTRODUCTION TO CRYPTOGRAPHY 14 (June 8, 2004), http://download.pgp.com/pdfs/Intro_to_Crypto_040600_F.pdf.

35. SCHNEIER, *supra* note 29, at 29.

36. *See* PGP CORP., *supra* note 34, at 12–13.

37. SCHNEIER, *supra* note 29, at 29.

38. *See, e.g.*, GPGTOOLS (Sept. 24, 2015), https://gpgtools.org (providing a download to easily add PGP encryption to Mac OS X e-mail).

39. *See, e.g.*, Milan Broz, *LUKS: Linux Unified Key Setup*, CRYPTSETUP (Sept. 5, 2016), https://gitlab.com/cryptsetup/cryptsetup/blob/master/README

So how does one go about bypassing encryption? Other than simply asking the target (or their acquaintances) for the password, which is likely to be a nonstarter,[40] law enforcement typically has four options: keyloggers, backdoors, brute-force attacks, and implementation flaws.[41] Keyloggers are straightforward: they are a piece of either hardware attached to the device or software running on the device which logs every key press.[42] The key presses are then either transmitted or the device eventually removed, and reviewed to find the encryption key. Backdoors are similarly conceptually simple, although from a public perception standpoint there is disagreement on what constitutes a backdoor.[43] As used herein (and in general by those in the technology industry), a backdoor is *any* modification to the encryption (whether for good, benign, or nefarious purposes) intended to enable access to the encrypted information by someone that does not have knowledge of the encryption key.[44] Brute-force attacks are simply guessing passwords until the correct one is found.[45] Given the complexity of passwords, however, this typically is not practicable.[46] Finally, implementation flaws are flaws inherent in how encryption is implemented, such that even when used correctly, the key can be exposed.[47] By their very nature, implementation flaws will vary from one implementation of encryption to the next.[48]

.md (last updated June 4, 2016) (describing LUKS, a whole-disk encryption program for Linux operating systems).

40. Unless the target is granted immunity, compulsion would violate the Fifth Amendment. *See infra* notes 176–83 and accompanying text.

41. *See* Declan McCullagh, *Feds Seek New Ways To Bypass Encryption*, CNET (Feb. 23, 2011), http://www.cnet.com/news/feds-seek-new-ways-to-bypass-encryption (providing examples of each).

42. *Spyware.Keylogger*, SYMANTEC (Feb. 13, 2007), https://www.symantec.com/security_response/writeup.jsp?docid=2004-033116-4256-99&tabid=2.

43. *See* Mario Trujillo, *The Slippery Definition of Encryption 'Back Doors*,' THE HILL (Feb. 17, 2016), http://www.thehill.com/policy/cybersecurity/269733-the-sliding-definition-of-encryption-backdoors.

44. *See id.*

45. McCullagh, *supra* note 41.

46. *See supra* note 32 and accompanying text. *But see* Michele Mosca, *Cybersecurity in an Era with Quantum Computers: Will We Be Ready?* 1, 1 (2015), https://eprint.iacr.org/2015/1075.pdf (noting that the advent of quantum computers may make brute forcing current encryption methods possible).

47. *See* McCullagh, *supra* note 41 (describing when computers decrypt a file system, the key is stored in the random access memory, and can potentially be accessed by computer forensics experts).

48. For example, in an effort to make Wi-Fi setup easier, the WPS protocol allows clients to connect by using an eight-digit pin with particular proper-

To summarize the technological discussion, there are a wide variety of methods by which law enforcement could attempt to access encrypted information. Source code speech issues arise only in the context of backdoors, because only they require modification of the written work of a developer or developers. Nevertheless, such backdoors are attractive, because of the limitations of other access methods (one must have access to install a keylogger, brute forcing may be computationally impracticable, and an implementation flaw may not exist). As a result, seeking to implement backdoors is a natural step for law enforcement to take to increase their information-gathering abilities.

B. A HISTORY OF ENCRYPTION REGULATIONS AND THE LIMITS ON THEM

In light of public availability of cryptography technology, as well as explosion of its usage in modern communications, the government has sought to regulate the dissemination of encryption technology.[49] Though laws regulating encryption technology predate modern computer equipment,[50] it was not until the 1990s that those laws were first challenged under the First Amendment.[51] Changes in the law in the early 2000s abruptly ended this debate,[52] at least in the courtroom setting. As a result, the extent to which limitations on the dissemination of encryption technology source code are permissible is still an open

ties. This dramatically reduces the universe of passwords to a mere 11,000 possibilities, and as a result of this implementation flaw, brute force attacks are possible. Stefan Viehböck, *Brute Forcing Wi-Fi Protected Setup*, WORDPRESS 4, 6 (Dec. 26, 2011), https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf (describing how the implementation flaw makes brute-force attacks possible); *Reaver-WPS-Fork-T6x*, GITHUB, https://github.com/t6x/reaver-wps-fork-t6x (last updated Sept. 26, 2016) (providing a download for software to execute the WPS brute-force attack).

49. Whitfield Diffie & Susan Landau, *The Export of Cryptography in the 20th and the 21st Centuries*, *in* THE HISTORY OF INFORMATION SECURITY 725, 726–28 (Karl de Leeuw & Jan Bergstra eds., 2007).

50. *Id.*

51. *See* Norman Andrew Crain, *Bernstein, Karn, and Junger: Constitutional Challenges to Cryptographic Regulations*, 50 ALA. L. REV. 869, 876–84 (1999) (discussing 1990s challenges to cryptographic regulations under the First Amendment).

52. *See* Diffie & Landau, *supra* note 49, at 732–33. At that point in time, encryption export was substantially deregulated, mooting challenges to limits on exportation. *See id.*

question. This Section introduces both past and present attempts to regulate encryption.

1. Past Legislative Responses to Encryption

Software backdoors would not be the government's first foray into the regulation of encryption technologies. Rather, since the Second World War (WWII), the government has restricted the exportation of encryption technologies to other countries on the basis that they were weapons.[53] More recently in the early 1990s, Congress attempted to entice companies to install hardware backdoors into all their communications products in an effort to gain the ability to easily intercept an electronic communication.[54]

Following WWII, cryptography was primarily a military technology.[55] As a result, each individual cryptographic device required an individual export license.[56] This policy continued through the end of the Cold War, at which point the NSA began approving the exportation of products utilizing encryption keys of limited length.[57] This loosening of restrictions did little to abate business pressure for the ability to export stronger encryption, and, in September of 1999, the government did away with most encryption-related export restrictions on retail products.[58]

In addition to export controls, in the early 1990s, the government sought to shape domestic use of encryption by proposing a device known as the Clipper Chip.[59] Framing the chip's implementation as voluntary, the government pushed companies to use the Clipper Chip as the means for embedding en-

53. *Id.* at 728.

54. Steven 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.

55. Diffie & Landau, *supra* note 49, at 728.

56. *Id.*

57. *Id.* at 729. Specifically, the NSA permitted keys of up to forty-bit length. *Id.* To put this in perspective, "an increase of one bit doubles the cost to the intruder," *id.*, and today the industry standard for Internet communications is 2048-bit keys. Liam Tung, *Google Strips Chrome, Android Trust for Symantec Root Certificate*, ZDNET (Dec. 14, 2015), http://www.zdnet.com/article/google-strips-chrome-android-trust-for-symantec-root-certificate. Thus, modern Internet communications are approximately $3*10^{604}$ times more difficult to crack than those that were secured by the Clipper Chip.

58. Diffie & Landau, *supra* note 49, at 732–33.

59. Levy, *supra* note 54.

cryption into their products.[60] The key, however (pun intended), was that, in addition to the chip containing the encryption key used by the parties to communicate, each Clipper Chip would encrypt each message with a second encryption key, kept by the government.[61] When authorized by a court order, the government could then easily intercept communications between any Clipper Chip-equipped devices.[62] Unfortunately for the government, the Clipper Chip never gained traction.[63] A combination of exposed security flaws in the chip, as well as the release of other tools based on open source encryption, shut down the Clipper Chip before it ever gained widespread use.[64]

2. Present Attempts To Control Encryption

After the fall of the Clipper Chip and the end of significant export regulation, encryption regulation largely became a non-issue. Since 2000, encryption usage has greatly proliferated, and in 2014, Apple took public-key encryption software and made it widely available to iPhone users,[65] exactly as described above.[66] As a result, even Apple became unable to access either information stored on the device or messages sent between two iMessage users.[67] In the wake of this action, the director of the FBI began calling for congressional action to require that Apple implement a backdoor that would enable government access to iPhones upon obtaining a court order.[68]

To date, however, no legislation has been introduced which would require the implementation of such backdoors. On April 13, 2016, however, the chair and vice-chair of the Senate Select

60. *Id.*

61. *Id.*

62. *Id.*

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

64. *Id.*

65. Bryan Chaffin, *FBI Cranky at Apple for Securing iOS, Only Has Itself (and NSA) To Blame*, MAC OBSERVER (Sept. 25, 2014), https://www.macobserver.com/tmo/article/fbi-cranky-at-apple-for-securing-ios-only-has-itself-and-nsa-to-blame.

66. *See supra* Part I.A.2.

67. Apuzzo et al., *supra* note 8.

68. Ryan J. Reilly & Matt Sledge, *FBI Director Calls on Congress To 'Fix' Phone Encryption by Apple, Google*, HUFFINGTON POST (Oct. 16, 2014), http://www.huffingtonpost.com/2014/10/16/james-comey-phone-encryption_n_5996808.html.

Committee on Intelligence did release a piece of draft legislation, which would require a technology company "that receives a court order from a government for information or data [to] (A) provide such information or data . . . in an intelligible format; or (B) provide such technical assistance as is necessary to obtain such information or data in an intelligible format or to achieve the purpose of the court order."[69] This requirement would apply to all communications, both foreign and domestic. Importantly, however, the act would not "authorize any government officer to require or prohibit any specific design or operating system to be adopted by any covered entity."[70] This limitation would seem to prohibit a law enforcement agency from demanding a backdoor. Although companies would be required to assist law enforcement when capable of doing so, the law would not require companies to change their products across the board. In other words, if a company could not (in general) hack their own product, the company *would not* have to change the product to make it always hackable, though they would have to make every attempt to hack a specific device when provided the device by law enforcement.[71]

In summary, several common strains can be drawn from various commentary that distinguish current calls for backdoors from the Clipper Chip and export controls of the past. First, unlike export controls, these backdoors would be applicable even to purely domestic technologies.[72] Second, unlike the

69. Compliance with Court Orders Act of 2016, 114th Cong. § 3(a)(1) (2016), http://feinstein.senate.gov/public/index.cfm?a=files.serve&File_id=5B990532-CC7F-427F-9942-559E73EB8BFB (discussion draft from Sen. Dianne Feinstein, Vice Chairman, S. Select Comm. on Intelligence).

70. *Id.* § 3(b).

71. Note that this is not the only way to read the bill. Other writers on encryption and the law have interpreted the text of the bill as requiring backdoors. *See, e.g.*, Joseph Donoso, *Anti-Encryption Bill Is an Affront to Privacy, Technological Security*, FREEDOMWORKS (Apr. 13, 2016), http://www.freedomworks.org/content/anti-encryption-bill-affront-privacy-technological-security; Riana Pfefferkorn, *The Burr-Feinstein Crypto Bill Would Gut Our Cybersecurity*, STAN. LAW. (Apr. 26, 2016), https://law.stanford.edu/2016/04/26/the-burr-feinstein-crypto-bill-would-gut-our-cybersecurity. I do not think this mandate is clear from the plain language of the draft, particularly given the "no required design or operating system" provision quoted above. I do agree, however, that the *intent* of the bill is likely to require backdoors, and I believe a clarification on that point will likely be included in a subsequent draft, should there be one. Such a broad mandate would, I argue *infra*, be inconsistent with the First Amendment. *See infra* Part II.C.

72. *See* Conor Friedersdorf, *Is Law Enforcement Crying Wolf About the Dangers of Locked Phones?*, THE ATLANTIC (Feb. 19, 2016), http://www

Clipper Chip, including such functionality would not be optional.[73] Third, also unlike the Clipper Chip, a modern backdoor would involve changes to developers' written product, rather than merely adding additional hardware.[74] As discussed below, it is this third difference in particular that raises many of the constitutional issues.

C. FREE SPEECH ISSUES OF FORCING SOFTWARE CHANGES

Software backdoors are not the first instance of encryption regulations potentially running afoul of the First Amendment. Rather, in the mid-1990s, both courts and commentators began considering to what extent the government could regulate the dissemination of source code.[75] At that point in time, however, the focus was largely on prior restraints of speech, whereas this Note focuses on limitations of compelled speech. This Section reviews this discussion to the extent it bears on present day calls for backdoors.

1. Doctrinal Limitations on Compelling Speech

When discussing First Amendment protection of speech, a common perspective among commentators is to consider whether the government is placing limitations on what can be said.[76] Indeed, the relevant text of the amendment—"Congress shall make no law . . . abridging the freedom of speech"[77]—facially suggests only that Congress may not abridge speech, but provides no explicit prohibition against Congress compelling speech. Nevertheless, the Supreme Court has rejected this literal interpretation of the First Amendment[78] and has recog-

.theatlantic.com/politics/archive/2016/02/is-law-enforcement-crying-wolf-about-the-dangers-of-locked-phones/470055.

73. *See* Reilly & Sledge, *supra* note 68.

74. *See* Laura Wagner, *Apple CEO Tim Cook: Backdoor to iPhones Would Be Software Equivalent of Cancer*, NPR (Feb. 24, 2016), http://www.npr.org/sections/thetwo-way/2016/02/24/468016377/apple-ceo-tim-cook-back-door-to-iphones-would-be-software-equivalent-of-cancer (quoting Apple's CEO as saying the only way to implement the backdoor desired would be to write software).

75. *See* Bernstein v. U.S. Dep't of State, 974 F. Supp. 1288, 1293 (N.D. Cal. 1977).

76. *See, e.g.*, WILLIAM W. VAN ALSTYNE, THE AMERICAN FIRST AMENDMENT IN THE TWENTY-FIRST CENTURY ix–x (4th ed. 2011) (showing a table of contents containing only one chapter on compelled speech and six chapters on other facets of First Amendment speech protection).

77. U.S. CONST. amend. I.

78. *See, e.g.*, Denver Area Educ. Telcomm. Consortium, Inc. v. FCC, 518

nized that the First Amendment also prohibits the state from compelling an individual or organization to speak.[79]

The Constitution provides a range of standards to apply when evaluating regulation of speech. The highest level, "the most exacting scrutiny," applies "to regulations that suppress, disadvantage, or impose differential burdens upon speech because of its content," while "regulations that are unrelated to the content of speech are subject to an intermediate level of scrutiny."[80] When strict scrutiny applies, the regulation of speech must be (1) "narrowly tailored" (2) "to a compelling state interest."[81] Finally, regulations on content "worthless or of *de minimis* value to society" receive only minimal scrutiny.[82] What level of standard to apply is the first step in determining what, if any, protection applies to a particular piece of speech.

In addition to these general principles, over the years, the Court has articulated several points of guidance regarding compelled speech that are relevant to mandating encryption backdoors. The first recognition of First Amendment protection from compelled speech came in 1943, when the Court held that "involuntary affirmation could be commanded only on even more immediate and urgent grounds than silence."[83] Such grounds are present "only when the expression presents a clear and present danger of action of a kind the State is empowered to prevent and punish."[84] In 1977, the Court recognized both that the state's interest must be "sufficiently compelling" to make compelled speech permissible,[85] and that one cannot be compelled to "contribute to the support of an ideological cause he may oppose."[86] Finally, in 1995, the Court recognized that "a narrow, succinctly articulable message is not a condition of

U.S. 727, 739–40 (1996) (rejecting the application of "literal[] categorical standards" in favor of "continual development" based on "new circumstances").

79. W. Va. State Bd. of Educ. v. Barnette, 319 U.S. 624, 633 (1943) (holding that the standard for compelling speech is even higher than that for censoring it).

80. Turner Broad. Sys. v. FCC, 512 U.S. 622, 642 (1994).

81. *Id.* at 680 (citing Boos v. Barry, 485 U.S. 312, 321 (1988)).

82. Yvonne C. Ocrant, Comment, *A Constitutional Challenge to Encryption Export Regulations: Software Is Speechless*, 48 DEPAUL L. REV. 503, 519–20 (1998) (quoting R.A.V. v. City of St. Paul, 505 U.S. 377, 400 (1992) (White, J., concurring)).

83. *W. Va. State Bd. of Educ.*, 319 U.S. at 633.

84. *Id.*

85. Wooley v. Maynard, 430 U.S. 705, 716 (1977).

86. Abood v. Detroit Bd. of Educ., 431 U.S. 209, 235 (1977).

constitutional protection."[87] Thus, a mandated expression may be something other than literal speech, and in such cases a mandate is impermissible unless there is a clear and present danger.[88]

Though the preceding discussion focuses on political or ideological statements, the Court has also been clear that the First Amendment's protection also prohibits compelled speech in non-political contexts,[89] albeit with a caveat not applicable to compelled software backdoors: commercial speech, or speech that "does no more than propose a commercial transaction," receives less protection than other forms of expression.[90] Thus, under the commercial speech doctrine, the government may require nutritional information,[91] warnings, or disclaimers on products.[92] Such a carve out is not applicable to software backdoors, however, because they do considerably more than "propose a commercial transaction."[93]

In summary, the First Amendment provides various levels of protection for speech, depending on the character of the speech. That protection extends not just to limits on speech, but also to laws that would compel speech. Finally, an act need not be literal speech to be protected.

2. Past Arguments on the Free Speech Status of Source Code

Around the same time that the Clipper Chip program was developing, both courts and commentators had begun considering whether the First Amendment protects computer source code as speech.[94] Although this question was never definitively

87. Hurley v. Irish-Am. Gay, Lesbian & Bisexual Grp. of Bos., 515 U.S. 557, 569 (1995) (finding seclection of parade participants to be protected by the First Amendment).

88. Professor Cass R. Sunstein has argued that the Court should reconsider the clear and present danger test. Cass R. Sunstein, *Opinion: In Face of Terrorism, Reassessing the First Amendment*, NORTHJERSEY.COM (Nov. 29, 2015), http://www.northjersey.com/opinion/opinion-guest-writers/in-the-face-of-terrorism-reassessing-the-first-amendment-1.1464277. To date, however, the Supreme Court has not moved in this direction.

89. *See, e.g.*, United States v. United Foods, Inc., 533 U.S. 405, 416 (2001) (striking down a required contribution to pay for mushroom advertising).

90. *Id.* at 409.

91. *E.g.*, N.Y. State Rest. Ass'n v. N.Y.C. Bd. of Health, 556 F.3d 114, 136 (2d Cir. 2009) (affirming denial of injunction against a law requiring calorie information in New York restaurants).

92. *See* Rubin v. Coors Brewing Co., 514 U.S. 476, 492 n.1 (1995).

93. *United Foods, Inc.*, 533 U.S. at 409.

94. *See* Bernstein v. U.S. Dep't of State, 974 F. Supp. 1288, 1293 (N.D.

settled by the courts,[95] following a series of three cases on the issue, various commentators developed arguments both in favor and against protecting source code under the Free Speech Clause of the First Amendment.[96] This Subsection reviews these arguments.

a. Arguments Supporting Free Speech Protection for Source Code

Prima facie, source code seems worthy of First Amendment protection. The First Amendment protects expression, and source code, among other things, allows programmers to express ideas to one another. Source code shares many of its characteristics with things that have been found to be protected, such as cookbooks.[97] Both contain, in written form, a mixture of English and numerical instructions.[98] Both may be published in a book.[99] Both require some level of training to be able to understand the information they contain.[100] More generally, both contain (what is intended to be) "truthful information."[101] Given our country's historical favoring of the expression of information,[102] this strongly suggests that source code, like other forms of technical instructions, should be protected.

Cal. 1997) (noting that Bernstein submitted his program for review in 1992).

95. *Compare Bernstein*, 974 F. Supp. at 1310–11 (finding export controls unconstitutional), *with* Karn v. U.S. Dep't of State, 925 F. Supp. 1, 11 (D.D.C. 1996) (upholding export controls as constitutional).

96. *See* Crain, *supra* note 51 (summarizing Junger v. Daley, 8 F. Supp. 2d 708 (N.D. Ohio 1998); Bernstein v. U.S. Dep't of State, 922 F. Supp. 1426, 1426 (N.D. Cal. 1996); and Karn, 925 F. Supp. 1.

97. *See* Sorrell v. IMS Health, Inc., 131 S. Ct. 2653, 2666 (2011) (listing a ban on the sale of cookbooks as the sort of action prohibited by the First Amendment).

98. *Compare* THE GOURMET COOKBOOK 852 (Ruth Reich ed., 2004) (containing instructions on how to make vanilla bean ice cream), *with* Captainbowtie, *PartAnalysisPane.java*, GITHUB (Dec. 2, 2015), https://www.github.com/captainbowtie/MockStats/blob/MockStats-1-(Swing)/PartAnalysisPane.java (containing instructions on how to calculate statistics for a mock trial competitor from information in a referenced database).

99. *Compare* THE GOURMET COOKBOOK, *supra* note 98, *with* GADDIS, *supra* note 16.

100. *Cf.* Linda Larsen, *How To Read a Baking Recipe*, ABOUT FOOD (Oct. 13, 2014), http://www.busycooks.about.com/od/howtobake/a/readabakingreci.htm (providing instructions on how to read a recipe).

101. *Cf.* Thompson v. W. States Med. Ctr., 535 U.S. 357, 374 (2002) (rejecting the argument that the government had an interest in restricting the flow of truthful information to prevent the public from making bad decisions with that information).

102. *See* Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555, 556 (1980)

At a more technical level, source code meets constitutional standards to be considered speech. The First Amendment protects both literal speech, spoken and written, as well as "inherently expressive" conduct.[103] Although not all written speech is protected,[104] source code falls within the sphere of protection. Unlike the picketing signs of *Giboney*[105] or the "White Applicants Only" sign referred to in *Rumsfeld*,[106] source code is not speech as a means to some illegal end. Rather, source code is, at least in some instances, intended primarily to have an expressive purpose, with any "conduct" resulting being merely incidental.[107] Although no court has ever ruled on the issue, *The Anarchist Cookbook* is likely protected,[108] despite teaching its readers how to make a bomb.[109] So, too, should source code be protected, even though it may enable its users to prevent the interception of their communications.

In addition to the expressive nature of source code, some commentators have advanced an independent "free speech values" argument.[110] Under this view, because source code facili-

(plurality opinion) (noting a history of openness).

103. Rumsfeld v. Forum for Acad. & Inst. Rights, Inc., 547 U.S. 47, 65–66 (2006) (analyzing whether conduct was inherently expressive after rejecting the argument that it was literal speech).

104. *Id.* at 62 ("[I]t has never been deemed an abridgment of freedom of speech . . . to make a course of conduct illegal merely because the conduct was in part initiated, evidenced, or carried out by means of language, either spoken, written, or printed." (quoting Giboney v. Empire Storage & Ice Co., 336 U.S. 490, 502 (1949))).

105. *Giboney*, 336 U.S. at 502.

106. *Rumsfeld*, 547 U.S. at 62.

107. This leaves open the cases where source code is not intended to be expressive. Additional arguments that source code is still worthy of protection, even in this instance, are raised in the next paragraph. *See also infra* Part III.B (discussing the problems that would arise in trying to assess whether source code was intended to be expressive on a case-by-case basis).

108. Tony Dokoupil, *After Latest Shooting, Murder Manual Author Calls for Book To Be Taken 'Immediately' out of Print*, NBC NEWS (Dec. 17, 2013), http://www.nbcnews.com/news/other/after-latest-shooting-murder-manual-author-calls-book-be-taken-f2D11758543 (quoting Brandenburg v. Ohio, 395 U.S. 444, 447 (1969)). *But see* Susan Jones, *Sen. Feinstein: 'Anarchist Cookbook' Not 'Protected by the First Amendment,'* CNSNEWS.COM (Apr. 3, 2015), http://cnsnews.com/news/article/susan-jones/sen-feinstein-anarchist-cookbook-not-protected-first-amendment.

109. WILLIAM POWELL, THE ANARCHIST COOKBOOK 113 (1971).

110. *See, e.g.*, Jorge R. Roig, *Decoding First Amendment Coverage of Computer Source Code in the Age of YouTube, Facebook, and the Arab Spring*, 68 N.Y.U. ANN. SURV. AM. L. 319, 326 (2012) ("If a particular activity is found to be . . . central to the development of a medium for the expression of ideas, then the court must engage in a comprehensive analysis of First Amendment val-

tates free speech, it is itself worthy of protection, even if source code is not itself speech.[111] The classic example is that of a movie projector.[112] The possession of a movie projector is itself clearly not an expressive or communicative act. Nevertheless, "[i]f the state were to prohibit the use of projectors without a license, First Amendment coverage would undoubtedly be triggered."[113] Indeed, the Sixth Circuit has held that regulations regarding the placement and designs of newspaper racks triggered First Amendment concerns.[114] Because source code, like film projectors or newspaper racks, is central to the development of the medium of the Internet and all its component communication technologies, it should likewise be protected under the First Amendment's guarantee of freedom of speech.[115]

b. Arguments Opposing Free Speech Protection for Source Code

Arguments against protection generally focus on rejecting the expressive nature of source code. Specifically, the argument takes the view that despite all the information source code may contain, it is ultimately just a tool for some further, not necessarily communicative, end.[116]

There are two components to this "lack of expression" argument. First, source code is the implementation of an idea, rather than the expression of the idea itself.[117] Put another way, unlike books or films, "source code is fundamentally different

ues . . . ."); *see also* Robert Post, *Encryption Source Code and the First Amendment*, 15 BERKELEY TECH. L.J. 713, 716 (2000) ("[The First Amendment] extends to forms of interaction that realize First Amendment values.").

111. Roig, *supra* note 110 ("Activities and devices that facilitate the development of a medium for the expression of ideas, though not themselves 'expressive,' trigger First Amendment coverage as readily as traditional speech.").

112. *See, e.g.*, Post, *supra* note 110, at 717 (giving the movie projector example); Roig, *supra* note 110, at 341–42 (framing the discussion in terms of Post's example).

113. Post, *supra* note 110, at 717.

114. *See* Plain Dealer Publ'g Co. v. City of Lakewood, 794 F.2d 1139, 1143 (6th Cir. 1986) (holding regulations to limit placement and design were an unconstitutional prior restraint on the freedom of the press).

115. Roig, *supra* note 110, at 345.

116. *See, e.g.*, Katherine A. Moerke, *Free Speech to a Machine? Encryption Software Source Code Is Not Constitutionally Protected "Speech" Under the First Amendment*, 84 MINN. L. REV. 1007, 1042–47 (2000) (arguing source code is not the expression of an idea, but merely the implementation of it).

117. *Id.* at 1044.

from these examples, whose primary function is expression. The function of source code is . . . to program a computer."[118] Although this form of implementing the idea may convey *some* information about the idea itself, "the First Amendment is not so broad as to protect all implementation of ideas."[119] Building off of this functionalist view of source code, the argument proceeds to analogize writing a computer program to building a machine.[120] Just as the building of certain devices may be restricted or outright prohibited without raising First Amendment concerns,[121] prohibiting the writing of particular types of source code also does not trigger First Amendment concerns.

In summary, encryption backdoors raise First Amendment questions because encryption software comes from source code, which is arguably communicative. Past attempts to regulate encryption have not resulted in a clear statement of whether that protection actually exists, nor have they addressed how mandated source code may differ from restraints on source code. The following Part addresses both of these questions.

II. EVADING ENCRYPTION: HOW MANDATED BACKDOORS IMPLICATE COMPELLED SPEECH CONCERNS

Given the government's history of regulating encryption, one might be led to believe that present calls for companies to include backdoors neatly fall into past treatment of encryption, and, like past efforts, should be permitted under the First Amendment, or at least be subject to similar analysis as export control regulations. Although there is substantial overlap between encryption regulations of the past and proposals for modern backdoors, requiring modern backdoors significantly differs from encryption programs of the past in several key aspects. This Part examines these differences and overlaps, highlighting aspects that lead to different First Amendment analysis than in the past. It then analyzes those First Amendment issues, showing how they play out for mandated software encryption backdoors.

118. *Id.*

119. *Id.* at 1045.

120. *See id.*

121. *See, e.g.*, 18 U.S.C. § 832(c) (2012) (prohibiting the building of a nuclear weapon).

A. DISTINGUISHING MANDATED SOFTWARE BACKDOORS FROM ENCRYPTION REGULATIONS OF THE PAST

As both calls for mandated backdoors and the programs described in Part I.B.1 involve the regulation of encryption, it may seem natural to assume that the legality of the present program turns on the legality of those past programs. However, though both past and present efforts involve the regulation of encryption, they differ in several key aspects that impact a constitutional analysis of calls for present-day regulation.[122]

Past attempts to curtail the release of encryption technologies can be largely broken into two programs. The first is the effort, beginning in the Cold War and continuing into the early 2000s, of the United States government to limit the exportation of encryption machines and software.[123] The second is the effort, initiated in the early 1990s but largely abandoned by the middle of that decade, to get United States technology companies to voluntarily integrate the Clipper Chip into their communications products.[124] The former differs from present regulations by applying only to software exports, while the latter differs because of its entirely voluntary nature.

The export ban of the second half of the twentieth century is distinguishable from proposed encryption backdoors because the export ban had a narrower focus. As the name suggests, the export ban focused solely on exports.[125] Although the constitutionality of even this narrow scope is doubtful,[126] assuming it is a valid prior restraint on speech, the much broader applicability of encryption backdoors to all domestic products calls for an independent analysis. This is both because the scope of the restriction is much larger (all products versus only exports) and because the interests of law enforcement and the general public likely receive different weights than they do in the export ban context. Furthermore, although the export ban and backdoors involve substantial overlap in regards to the free speech analysis that applies, the export ban was a prior restraint on speech,[127] while backdoors implicate compelled speech concerns. As a result of these differences, the analysis of encryption

122. *See infra* Part III.A.

123. Diffie & Landau, *supra* note 49, at 728.

124. Levy, *supra* note 54.

125. *See* Diffie & Landau, *supra* note 49.

126. *See, e.g.*, Bernstein v. U.S. Dep't of State, 974 F. Supp. 1288, 1310–11 (N.D. Cal. 1997) (holding unconstitutional several of the export controls).

127. *Id.* at 1310.

backdoors involves considering a wider variety of law enforcement tools. There is only one way to stop the spread of information: limiting the communication of that information. However, there are several ways to gain access to information beyond requiring broad encryption backdoors.[128]

Turning to the Clipper Chip, mandatory encryption backdoors are fundamentally different than the voluntary Clipper Chip encryption "solution" suggested in the 1990s. Unlike present calls for "mandatory" backdoors, the Clipper Chip program was never required.[129] Instead, it was billed as an optional tool for companies to easily integrate encryption into their products.[130] Given this entirely optional nature, the Clipper Chip raised none of the *compelled* speech issues that backdoors raise. As a result of these differences between both the export control programs and the Clipper Chip, legal analysis of these past programs does not necessarily imply similar results for a modern backdoor mandate.

B. ANALYZING WHETHER SOURCE CODE CONSTITUTES SPEECH UNDER THE FIRST AMENDMENT

Despite the differences outlined above, modern calls for encryption backdoors and the export restrictions of the past do have one thing in common: both seek to regulate computer source code.[131] Whether or not source code is even protected by the First Amendment has been a point of contention since the late 1990s, and the courts of that era never came to a uniform conclusion.[132] Furthermore, with the end of the export ban in

128. *See infra* Part III.B (discussing how investigators can gain access to communications without infringing on the First Amendment).

129. *Compare* Shane Harris, *Feds Want 'Backdoor' into Phones, While Terrorists Walk Through Front Door*, DAILY BEAST (Nov. 30, 2015), http://www.thedailybeast.com/articles/2015/11/30/feds-want-backdoor-into-phones-while-terrorists-walk-through-front-door.html (noting renewed calls to restrict encryption technology), *with* Levy, *supra* note 54 (noting the voluntary nature of the Clipper Chip).

130. Levy, *supra* note 54.

131. *Compare Bernstein*, 974 F. Supp. at 1306 (analyzing the exportation of source code), *with* Trevor Timm, *Weak Encryption Won't Defeat Terrorists — But It Will Enable Hackers*, THE GUARDIAN (Dec. 10, 2015), https://www.theguardian.com/commentisfree/2015/dec/10/weak-encryption-wont-defeat-terrorists-but-it-will-enable-hackers (discussing encryption tool's source code regarding modern backdoors).

132. *Compare Bernstein*, 974 F. Supp. at 1310–11 (finding export controls unconstitutional), *with* Karn v. U.S. Dep't of State, 925 F. Supp. 1, 10 (D.D.C. 1996) (upholding export controls as constitutional).

the early 2000s, the debate became largely academic.[133] As a starting point, First Amendment protection for source code is a necessary condition for encryption backdoors to raise compelled speech concerns. The debate over the applicability of the First Amendment to source code continues to this day, with increased fervency as the Internet has come to play a significant role in the average American's life. This Section analyzes past commentators' consideration of this issue,[134] arguing that source code ought to fall within the protections of the First Amendment. Part I.C.2 introduced arguments both for and against protecting source code under the First Amendment. An analysis of these arguments indicates that source code ought to be protected, though for different reasons in different cases.

As a starting point, it is fairly uncontroversial that if a piece of source code is expressive, it should be protected. Even writers that believe source code should not be protected agree that *if* it was expressive, it would be worthy of protection.[135] Thus, in instances where source code is intended to communicate an idea, source code should be protected as itself communicating that idea.

In other instances, however, detractors are correct to point out that source code was written not to communicate an idea, but entirely as a tool to enable a machine to carry out a task. In these instances, the "expressive content" argument in favor of First Amendment protection does not stand up to scrutiny. However, it can be very difficult to distinguish the purpose for which a particular piece of source code was written.[136] Nevertheless, assuming the purpose can be distinguished, in cases where a solely non-communicative purpose can be determined, advocates for First Amendment protection can fall back to the "First Amendment Values" argument, which, in the context of source code for communication products (which encryption clearly falls into), will almost universally be persuasive.

133. *See* Diffie & Landau, *supra* note 49, at 732–33.

134. *See supra* Part I.C.2 (introducing these issues).

135. *See, e.g.*, Moerke, *supra* note 116, at 1029 (suggesting that if source code was "written to make a statement" it would be protected speech).

136. This difficulty is discussed in more detail in a later paragraph in this Section.

1. The "Expressive Content" Argument Covers Most Source Code

When the First Amendment classification of source code was last considered in earnest, Internet usage was in its infancy.[137] In 1997, less than half the country had Internet access in the home.[138] Groups advocating for the publishing of source code were uncommon at that time. For example, the Open Source Initiative, a leading group in such advocacy, was not founded until 1998.[139] As a result, it (perhaps) made sense to say that source code was non-communicative at that time, because it was unlikely that source code would be communicated to a large audience. This is no longer the case. Though developers may publish source code for many reasons, one reason is to "*understand* [a program's] functioning."[140] Such a goal suggests that the source code itself, even if it is the particular implementation of an idea, still performs an educative function: teaching other individuals how a computer program functions as well as how they could implement it themselves. Such educative materials fall within the ambit of First Amendment protections and thus cover open source software code.[141]

This treatment of open source code, however, leaves a noteworthy gap in the universe of source code's protection. First, although many of the encryption technologies at issue are open source,[142] the most well-known instance is not.[143] Though

137. *Cf.* THOM FILE & CAMILLE RYAN, U.S. CENSUS BUREAU, U.S. DEP'T OF COMMERCE, COMPUTER AND INTERNET USAGE IN THE UNITED STATES: 2013 1 (2014) (documenting the rise of Internet usage between the mid-1980s and 2013).

138. *Id.* at 4.

139. *History of the OSI*, OPEN SOURCE INITIATIVE (Sept. 2012), http://opensource.org/history.

140. Richard Stallman, *Why Free Software Is More Important Now than Ever Before*, WIRED (Sept. 28, 2013) (emphasis added), https://www.wired.com/2013/09/why-free-software-is-more-important-now-than-ever-before.

141. Joseph Burstyn, Inc. v. Wilson, 343 U.S. 495, 501 (1952) (finding First Amendment coverage for things that teach doctrine).

142. Indeed, this open source nature limits the effectiveness of backdoor regulations, even if the government could constitutionally mandate them. *See* Timm, *supra* note 131.

143. Specifically, Apple's iMessage system, which encrypts messages sent between two iPhone users, is not. *See* Daniel Eran Dilger, *EFF Ranks Apple's iMessage, FaceTime "Best Mass Market Options" for Secure Messaging, Ahead of BlackBerry Messenger, Google Hangouts, Facebook, Microsoft Skype*, APPLEINSIDER (Nov. 5, 2014), https://www.appleinsider.com/articles/14/11/05/eff-ranks-apples-imessage-facetime-best-mass-market-options-for-secure-messaging-ahead-of-blackberry-messenger-google-hangouts-facebook

the First Amendment applies to intrusions into the internal writings of a group just as much as to public writings,[144] there still remains a gap in code covered by the First Amendment: source code that is not intended to be communicative. The argument against treating source code as expressive carries the most weight at this point: if the source code is not intended to convey information to others, then it does not seem plausible to say that it triggers any First Amendment concerns. Although this line of reasoning has theoretical appeal, it presents a large practical problem: How does one distinguish between expressive and non-expressive code? For small programs, it may be possible to query the program author and simply ask their intentions. Such an approach for larger programs, however, is implausible. The Linux kernel (the core component of many major operating systems), for example, has had almost 12,000 developers contribute to its source code since 2005.[145] Contacting each and every one of those developers would be an exercise in futility. At best, a court could speculate as to developer intent, based on the nature of the software, its development philosophy, and any other indirect evidence that makes a particular intention more or less likely to be present in that particular case. Such an approach, however, would necessarily be an approximation.

2. The "Free Speech Values" Argument Covers All Encryption Software Not Addressed by the "Expressive Content" Argument

Even if this hurdle could be overcome, and every developer could (truthfully) indicate that they did not intend to express any idea when writing their code, there would still remain the "free speech values" argument. Few writers have developed counterarguments to this line of thought other than to merely presume the negative—that constructions which facilitate speech are not themselves protected by the First Amendment.[146]

-microsoft-skype.

144. *See* Boy Scouts of Am. v. Dale, 530 U.S. 640, 648 (2000) (noting intrusion into "internal structure or affairs of an association" may impinge on First Amendment freedoms (quoting Roberts v. U.S. Jaycees, 468 U.S. 609, 623 (1984))).

145. JONATHAN CORBET ET AL., LINUX KERNEL DEVELOPMENT: HOW FAST IS IT GOING, WHO IS DOING IT, WHAT ARE THEY DOING AND WHO IS SPONSORING THE WORK 2 (2015).

146. *See, e.g.*, Ocrant, *supra* note 82, at 540 (stating that the "motors, levers, gears and wires" of a newspaper printer are not protected by the First Amendment).

Such a view, however, is unsupported by Supreme Court interpretations of the First Amendment, which have extended protection to activities beyond pure speech into "conduct commonly associated with [speech]."[147]

This combination of the "expressive content" argument and the "free speech values" argument collectively bring most source code within the coverage of the First Amendment. Nevertheless, such a rationalization for protection will still not protect *all* source code, but rather only source code that is intended as communicative or related to communications. This leaves a noteworthy gap, specifically for non-communicative devices. Though such a gap may seem problematic for First Amendment protection at first glance, in reality, its effect is very minimal as regards the present encryption backdoor debate. Thus far, the information sought by law enforcement has been chiefly communications.[148] Thus, for the purposes of the present description of encryption backdoors, the combination of the two arguments covers all the source code at issue.

In summary, in the Internet-connected age, source code will generally be expressive enough to warrant potential First Amendment protection, because much of source code, though written primarily to control a computer, is also written with the goal of communicating valuable information to other developers. Furthermore, to the extent a particular piece of code is not expressive, in the communication context (with which encryption is necessarily concerned) its potential for protection will still be supported by the "Free Speech Values" argument, as source code that makes encryption possible is a tool that readily contributes to making the communication of expressive content possible.

C. ANALYZING BROAD BACKDOORS: STRICT SCRUTINY DOES NOT PERMIT UNIVERSAL BACKDOORS

Given that source code falls within the protection of the First Amendment, this Section examines whether or not laws requiring backdoor implementation would nevertheless be permissible. Applying the First Amendment jurisprudence described in Section I.C, it concludes that universal encryption backdoors as desired by individuals like the FBI Director would

147. City of Lakewood v. Plain Dealer Publ'g Co., 486 U.S. 750, 759 (1988).

148. *See* Thomas, *supra* note 2 (noting the FBI was being challenged by "encrypted *communications*" (emphasis added)).

impermissibly require compelled speech even in the presence of a specific "clear and present danger."

Just because source code is protectable by the First Amendment does not mean that compelled encryption backdoors are necessarily unconstitutional. In the prior restraint arena, for instance, content such as child pornography has triggered a First Amendment analysis, but prohibiting its distribution was constitutionally permitted nevertheless.[149] This Part first analyzes what level of scrutiny should be applied to encryption backdoors, and then, having concluded that strict scrutiny applies, argues that under no circumstances would the broad-sweeping backdoors being sought be permitted under the First Amendment.

1. Strict Scrutiny Applies to Encryption Backdoors

As noted in Part I.C.1, the Constitution provides a range of standards to apply when evaluating regulation of speech. As an initial matter, source code clearly does not fall within the treatment of the commercial speech doctrine. Commercial speech is limited to speech that "does no more than propose a commercial transaction."[150] Source code is not such a proposal, but rather instructions on how to perform a particular task.

Additionally, strict scrutiny or intermediate scrutiny applies unless the content of speech is worthless to society.[151] Communicating how to implement strong encryption has worth to society. Without it, the development secure software would be greatly hindered, and everything from bank records to medical information would be vulnerable to attack.[152]

The more interesting (and difficult) question is whether regulations of encryption source code should receive intermedi-

149. New York v. Ferber, 458 U.S. 747, 774 (1982).

150. United States v. United Foods, Inc., 533 U.S. 405, 409 (2001).

151. Ocrant, *supra* note 82 (quoting R.A.V. v. City of St. Paul, 505 U.S. 377, 400 (1992) (White, J., concurring)).

152. *See* Cory Doctorow, *Encryption Won't Work If It Has a Back Door Only the 'Good Guys' Have Keys to*, THE GUARDIAN (May 1, 2015), https://www.theguardian.com/technology/2015/may/01/encryption-wont-work-if-it-has-a-back-door-only-the-good-guys-have-keys-to. *But see* Ocrant, *supra* note 82, at 542. After arguing that source code should not receive any protection, Ocrant concedes that if it is protected, regulations of source code should receive only minimal scrutiny. *Id.* This argument is based, however, on the reasoning that because it should not receive strict or intermediate scrutiny, it must default to minimal scrutiny. *Id.* at 541–42. Ocrant does not analyze what makes encryption source code "worthless to society." *See id.* at 542.

ate scrutiny or strict scrutiny. In cases of restraints on speech, the "principal inquiry in determining content neutrality . . . is whether the government has adopted a regulation of speech because of disagreement with the message it conveys."[153] Compelled speech, however, adds a wrinkle to this inquiry, because the government is not trying to censor a message with which it disagrees, but rather trying to modify the message to suit the government's own end. Nevertheless, the Court has been clear that the same level of scrutiny applies to compelled speech as to compelled silence (prior restraints).[154] The inquiry, therefore, when the government is attempting to compel a particular message, could be characterized as whether the government has adopted a regulation requiring speech because the government seeks to force the conveyance of a particular message.

There is not a straightforward answer to this question. No court has directly addressed the issue of compelled source code speech, and those that have addressed the issue of restraints on source code speech have come out on both sides.[155] Here the distinction between prior restraints of the past and the compelled nature of backdoors today comes into play. Unlike the prior restraint at issue in *Bernstein*, encryption backdoors would require the expression of a particular idea, specifically "this is how you encrypt information *and here is a backdoor to allow the government access to that information*." The emphasized portion is a particular message that the software author (presumably) does not wish to convey, but is being compelled to do so by government regulation. This makes such regulation content-specific, as it is a regulation based on "[agreement or disagreement] with the message it conveys."[156]

153. Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989).

154. *See, e.g.*, Riley v. Nat'l Fed'n of the Blind of N.C., Inc., 487 U.S. 781, 796–97 (1988) ("There is certainly some difference between compelled speech and compelled silence, but in the context of protected speech, the difference is without constitutional significance, for the First Amendment guarantees freedom of speech, a term necessarily comprising the decision of both what to say and what *not* to say.").

155. *Compare* Karn v. U.S. Dep't of State, 925 F. Supp. 1, 10 (D.D.C. 1996) (finding export restriction to be a content-neutral regulation because "[t]he defendants are not regulating the export of the diskette because of the expressive content of the comments and or source code, but . . . because of the belief that . . . it [is] easier for foreign intelligence sources to encode their communications"), *with* Bernstein v. U.S. Dep't of State, 974 F. Supp. 1288, 1307 (N.D. Cal. 1997) (finding export restriction to be subject to strict scrutiny).

156. Turner Broad. Sys. v. FCC, 512 U.S. 622, 642 (1994) (quoting Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989)).

As a content specific regulation, encryption backdoors must withstand strict scrutiny. Such regulations must "promote a compelling interest" through "the least restrictive means to further the articulated interest."[157] Although not free from doubt, there is a likely a compelling interest in requiring encryption backdoors, because they have the potential to reduce crime.[158] This doubt arises because there is at least *some* reason to believe that requiring encryption backdoors would have little to no effect on the actual encryption used by criminals.[159] It may be the case that if encryption backdoors are implemented into products made by companies responsive to regulation, criminals would simply move to using tools from darker parts of the Internet that are less responsive to regulation.[160] Nevertheless, while the extent to which such regulation would be effective is questionable, it would likely have at least some margin of impact. For example, in November 2015 terrorists in France coordinated their attack (ultimately killing 130 people) using unencrypted text messages that could have been intercepted without any encryption backdoors,[161] but one can easily imagine them using encrypted iMessages instead,[162] just as the San Bernardino attackers did. If that had been the case, then only with backdoors present would the government have been able to intercept their messages.

157. Sable Commc'ns of Cal., Inc. v. FCC, 492 U.S. 115, 126 (1989).

158. *See* David Auerbach, *There Is No Good Argument for Encryption Backdoors*, SLATE (Nov. 19, 2015), http://www.slate.com/articles/technology/bitwise/2015/11/encryption_backdoors_won_t_make_us_safer_from_terrorism_john_brennan_john.html.

159. *See id.* ("If secure encryption is outlawed, only outlaws will have secure encryption."). Although only tangential to a constitutionality discussion, as a practical matter, it is of significant, if not overriding, importance that were encryption backdoors actually implemented, criminals of any skill would simply shift to using already-existing open source programs that do not have any backdoors. *See id.*

160. *See id.*

161. Dan Froomkin, *Signs Point to Unencrypted Communications Between Terror Suspects*, THE INTERCEPT (Nov. 18, 2015), https://theintercept.com/2015/11/18/signs-point-to-unencrypted-communications-between-terror-suspects.

162. *Cf.* Mike Elgan, *Why It's Time for Apple To Open FaceTime*, CULT OF MAC (Sept. 28, 2013), http://www.cultofmac.com/247673/why-its-time-for-apple-to-open-facetime (noting users could switch between SMS and iMessage "without thinking about it").

2. Broad Encryption Backdoors Do Not Survive a Strict Scrutiny Analysis

Despite promoting a compelling government interest, wide-sweeping encryption backdoors meet a fatal flaw when considering whether or not they are narrowly tailored to achieve the government's interest. Every day, over six-billion text messages are sent.[163] The vast majority of these communications are (one would hope) not communications between terrorists. Nevertheless, each and every one of these communications would be subject to backdoor access. Putting aside the massive privacy concerns that has the potential to raise,[164] such access is not "narrowly tailored" to achieve the government's interest. In a related context, the Supreme Court has struck down laws restricting speech on the basis that they were not narrowly tailored to preventing "advocacy . . . directed to inciting or producing imminent lawless action."[165] Similarly, in the context of encryption backdoors, any effective law requiring the installation of backdoors would invade into the sphere of communications where there is no government interest in having backdoor access. To pass constitutional muster, the law would have to be so narrow as to be of very limited effect in gaining access to communications, but in order to be effective, the law would necessitate adding backdoor access to communications where there is no compelling government interest.

III. CONFRONTING COMPULSION: HOW COURTS AND LAW ENFORCEMENT SHOULD TREAT REQUESTS FOR ENCRYPTED COMMUNICATIONS

Given that source code falls within the protection of the First Amendment, this Part examines what means are left to investigators for accessing encrypted information. Although laws requiring broad backdoors would likely violate the First Amendment, there are strong public policy considerations favoring alternatives that would support law enforcement objec-

163. Michael O'Grady, *SMS Usage Remains Strong in the US: 6 Billion SMS Messages Are Sent Each Day*, FORRESTER (June 19, 2012), http://www.blogs.forrester.com/michael_ogrady/12-06-19sms_usage_remains_strong_in_the_us_6_billion_sms_messages_are_sent_each_day.

164. *See generally* Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, 8 J. TELECOMM. & HIGH TECH. L. 359 (2010) (discussing the privacy implications of government backdoors).

165. Brandenburg v. Ohio, 395 U.S. 444, 447 (1969) (per curiam).

tives requiring access to encrypted information. This Part presents two technological solutions that pass First Amendment muster, as well as an acknowledgement that in at least some circumstances, law enforcement may be left, as in the case of encryption and the Fifth Amendment, with having to make do without the information desired. This Part then makes several preliminary suggestions for a statutory framework that could implement the stronger of these two solutions, and concludes by addressing counterarguments to the proposed solution.

A. WHAT'S AN INVESTIGATOR TO DO? GETTING AT COMMUNICATIONS WITHOUT VIOLATING THE FIRST AMENDMENT

In light of the preceding discussion, it may appear that investigators are stuck between a rock and a hard place. Backdoors would either be too constrained to be effective or too broad to be constitutional. However, there are responses to this dilemma that satisfy both technological and constitutional requirements. This Section introduces some of these possible solutions. Notably, the solutions proposed are somewhat consistent with the draft Compliance with Court Orders Act of 2016 language, at least as I interpret it.[166] The solutions below do not require changes to a company's product *en masse*, but do require steps to be taken in particular circumstances. Although they admittedly do not provide the coverage that comprehensive encryption backdoors would provide, these solutions may serve as a starting point for examining further tools that would aid law enforcement while still respecting the boundaries put in place by the Constitution.

1. Permitted Compelled Speech: Utilize Existing Technological Limitations in Encryption Products To Obtain the Desired Information on an Individual Basis

Although the encryption of a communication may be unbreakable, attempting to insert backdoors to make it breakable is not the only way to gain access to communications.[167] There

166. *See supra* note 71 (discussing differing interpretations). Note that under the reading some other authors have given the draft language, the proposed solutions *would not* be consistent with the Act, as they read the Act as mandating universal backdoors, which, as discussed *supra*, are not permissible under the First Amendment.

167. For example, it is possible to trick someone into downloading what appears to be a software update, but what in actuality is a program that intercepts communications before they are encrypted. *See, e.g.*, Michael Kassner,

are other ways of gaining access to information stored on an encrypted device that can be more narrowly tailored, so as to pass the strict scrutiny of the First Amendment. What follows are two possible responses targeted at the iPhone[168] that would satisfy the narrow tailoring requirement. Under circumstances where probable cause exists, a court could order a company to take either of the proceeding actions to assist in carrying out a warrant, without running against the First Amendment.

a. Man-in-the-Middle Attacks: Intercepting "Live" Communications

The first vulnerability law enforcement could use to obtain live access to communications is a man-in-the-middle (MITM) attack. This vulnerability is so named because the interceptor "stands" in the middle of the two communicating parties, deceiving both the sender into believing the message is going directly to the recipient and the receiver into believing the message is coming directly from the sender.[169] In the case of a system like iMessage, because Apple controls its encryption key infrastructure, it could surreptitiously use encryption keys provided by the government to effect its encryption, with the send-

Malware Poses as Software Updates: Why the FBI Is Warning Travelers, TECHREPUBLIC (May 14, 2012, 12:55 AM), http://www.techrepublic.com/blog/it-security/malware-poses-as-software-updates-why-the-fbi-is-warning-travelers.

168. This discussion centers on the iPhone given its prominence in news coverage regarding law enforcement access to encrypted information. These forms of intercept could be converted to other communications media, subject to the caveats described in the discussion.

169. TOM'S GUIDE Staff & Ryan Goodrich, *What Is a Man in the Middle Attack?*, TOM'S GUIDE (Oct. 23, 2013), http://tomsguide.com/us/man-in-the-middle-attack,news-17755.html. To go into a bit more detail, suppose Eve wants to intercept a message sent from Alice to Bob. Ordinarily, Alice would be able to send a secure message to Bob by finding Bob's public key, using that key to encrypt her message, and then sending the message to Bob. Only Bob would be able to decrypt the message, by using his private key. In an MITM attack, Eve impersonates Bob (generally by having a privileged position such that when Alice looks online for Bob's public key, she unknowingly gets Eve's instead). Then when Alice encrypts her message, she uses Eve's key instead of Bob's. Eve intercepts the message in transit, and because it was encrypted with her public key, Eve can use her private key to decrypt it. After reading the message, Eve can re-encrypt the message using Bob's real public key and send the message onto him, with neither Alice nor Bob any the wiser. *See* Matthew Copeland et al., *The GNU Privacy Handbook*, GNUPG (1999), https://www.gnupg.org/gph/en/manual.html (discussing information utilized in the example under the chapter 3 heading).

er and receiver being none the wiser.[170] Doing this for all iPhone users would raise the same narrow tailoring concerns as broad encryption backdoors. However, for specific individuals (based on information that the individual's communications are related to a criminal investigation sufficient to allow a warrant to issue) such an approach would not raise overbreadth concerns. It is, however, worth noting that while such an approach would grant access to systems like iMessage, where there is some central authority managing the encryption key infrastructure, it would be inapplicable to a distributed key system.[171] Additionally, such an attack would be capable of intercepting only communications sent from the point in time when the man-in-the-middle position is established.[172] Unless past communications were sent over the (now compromised) channel, there would be no way to intercept them.[173]

b. Custom-Crafted Updates: Compelled Speech That Is Sufficiently Narrowly Tailored

As a result of the aforementioned limitations, law enforcement may desire additional tools to access communications that a man-in-the-middle attack does not cover. Fortunately for them, Apple's (and other cellphone vendor's) privileged position provides such a solution. As the operating system developer for the iPhone, Apple has a great deal of control over the software on it, including the software updates. On other platforms, malicious software updates have been used to compromise computer security integrity.[174] Given the closed nature of iOS, Apple could implement such an update either without any notification to

170. *See* Dennis Fisher, *Apple iMessage open to Man in the Middle, Spoofing Attacks*, THREATPOST (Oct. 17, 2013), https://threatpost.com/apple-imessage-open-to-man-in-the-middle-spoofing-attacks/102610; *see also supra* Part I.A.2 (discussing the technicalities of encryption key systems). Replace Alice, Bob, and Eve with iPhone User 1, iPhone User 2, and Apple, respectively, in the example *supra* note 169, and that example is precisely what the government could require.

171. This approach is inapplicable because such an MITM attack relies on the privileged position of the directory operator to be able to transparently alter the public keys it provides when people request them. *See* Fisher, *supra* note 170 (noting that systems "without a central directory" would not be vulnerable to this type of attack).

172. *See* TOM'S GUIDE Staff & Goodrich, *supra* note 169 (noting that man-in-the-middle attacks are limited to communications exchanged after the relay between the two parties is established).

173. *See id.*

174. Kassner, *supra* note 167.

the user or as an innocuous update that hides its true purpose.[175] Once installed, such an update could grant access to past encrypted communications, as well as any other information saved on the phone.[176] As was the case with man-in-the-middle attacks, while such action may raise broadness problems if applied to all users, when only requested for specific individuals, such an attack likely satisfies the narrow tailoring requirements of the First Amendment.[177]

2. Beyond Compelled Speech: Find Other Ways To Get the Information or Do Without It

Although the suggestions above provide some possibilities for access to encrypted information, they are still imperfect solutions. Both rely on the privileged position of a particular party in order to gain access to communications, and, as the examples make clear, that privileged position simply does not exist for all communications. In such cases, it may simply be the case that an investigator must make do with the information obtainable by constitutional means, just as is the case with more traditional forms of evidence gathering.

The reality that some evidence is simply beyond the constitutional reach of investigators is not a new idea. Indeed, despite computer encryption's relative novelty, there are already several cases in the Fifth Amendment context from which to draw parallels in regards to access to encrypted information.[178] These cases support the view that when it comes to encryption, there may simply be some cases where investigators cannot get

175. *Cf.* J. O'Dell, *Linux Chief: 'Open Source Is Safer, and Linux Is More Secure than Any Other OS' (Exclusive)*, VENTUREBEAT (Nov. 26, 2013), http://venturebeat.com/2013/11/26/linux-chief-open-source-is-safer-and-linux-is-more-secure-than-any-other-os-exclusive/ (noting that closed source programs are vulnerable to having backdoors implemented without consumer knowledge).

176. *See* Juli Clover, *'Masque Attack' Vulnerability Allows Malicious Third-Party iOS Apps To Masquerade as Legitimate Apps*, MACRUMORS (Nov. 10, 2014), http://www.macrumors.com/2014/11/10/masque-attack-ios-vulnerability.

177. Of course, such an attack would also have to satisfy the privacy requirements of the Fourth Amendment, as well as the statutory requirements of the Electronic Communications Privacy Act. *See generally* WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW 340–63 (2016) (discussing the legal requirements for law enforcement to intercept electronic communications and access stored communications).

178. *See, e.g.*, United States v. Kirschner, 823 F. Supp. 2d 665, 668–69 (E.D. Mich. 2010) (finding that compelling a defendant to reveal his encryption password amounts to self-incrimination).

at the information desired. Although circumstances have led to alternative outcomes in some cases,[179] in some instances, courts have recognized that a defendant cannot be compelled to turn over her password, even when the failure to do so effectively cuts off a key source of information.[180] Though law enforcement can overcome this issue by granting a suspect immunity,[181] in some cases, only the primary key password holder may be the person the government wants to charge. In such cases, the only recourse is to seek the password information from another person with knowledge of it.[182]

Similarly, in regards to communication backdoors, if investigators are unhappy with the limited compelled speech options constitutionally available to them, they must either find a permissible means of obtaining the information (through the permitted technical solutions described above or through less technical means such as getting the suspect's cooperation in accessing the encrypted information) or simply do without it. Furthermore, unlike the Fifth Amendment context, no grant of immunity can remedy the situation. While such a grant allows for the protection of the interests implicated by the Fifth Amendment by preventing the disclosure or information derived from it from being used against the individual making the statement,[183] a grant of immunity does not resolve the First Amendment issue. Grants of immunity do not protect the interest of a speaker being able to control the content of his or her message, and thus, unlike in the context of the Fifth Amendment, they cannot convert an unconstitutional backdoor into a constitutional one.

B. WORKING TOWARDS A TECHNICAL SOLUTION: STEPS TO TAKE TOWARDS ACHIEVING NARROWLY TAILORED BACKDOORS

Of the two solutions proposed, narrowly tailored backdoors would permit access to more information, allowing access not

179. *See, e.g.*, United States v. Fricosu, 841 F. Supp. 2d 1232, 1237 (D. Colo. 2012) (noting that where "the government knows of the existence and location of the computer's files" there is no Fifth Amendment protection).

180. *See, e.g.*, *In re* Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335, 1352–53 (11th Cir. 2012) (recognizing a Fifth Amendment right to not turn over encryption password).

181. *See* Kastigar v. United States, 406 U.S. 441, 461 (1972).

182. *See, e.g.*, United States v. Buckner, 473 F.3d 551, 556 (4th Cir. 2007) (upholding search of a computer conducted after defendant's wife gave law enforcement the password).

183. *See* Ullmann v. United States, 350 U.S. 422, 431 (1956).

just to communications transmitted after access is established but also to past communications stored on a device.[184] Thus, when possible, narrowly tailored backdoors better services the public interest law enforcement is attempting to vindicate when it seeks to gain access to an encrypted device. This Section proposes statutory structure that would aim to make such an access regime possible.

As a first step toward implementing the proposed solution, Congress should work with technology companies and law enforcement to develop a formal structure for requesting device access. Currently, no such framework exists, and, as law enforcement's attempts to nevertheless force cooperation in the San Bernardino case suggest,[185] the absence of such a framework makes it difficult for law enforcement to easily gain access when needed and legitimizes technology companies' concerns about establishing bad precedent.[186]

Determining the precise contours of this framework is beyond the scope of this Note, as it involves weighing such detailed concerns as industry costs, new technological developments, privacy concerns, and data transfer logistics well beyond those discussed thus far. Nevertheless, a few broad key features may be suggested. First, to conform with the narrow tailoring requirement, device manufacturers should be able to limit the backdoor they provide to a singular, specific device. Perhaps this takes the form of custom crafting access based on unique identifying information about the device, or perhaps it involves law enforcement turning over the device to a manufacturer, so that the government never has possession of the backdoor mechanism itself. In either event, it is key that the manufacturer be able to maintain limits on the backdoor, as any broader use beyond that required to resolve the "clear and present danger" of lack of access would go beyond the narrow requirements of the situation.

Second, it may be useful to base the foundation of this framework on that laid out in other electronic search contexts.

184. *See supra* Part III.A.1.

185. *See* Krishnadev Calamur, *Apple vs. the FBI*, THE ATLANTIC (Feb. 17, 2016), http://www.theatlantic.com/national/archive/2016/02/apple-fbi-san-bernardino/463128/.

186. *See id.* (laying out both the government's argument for the need of access and Apple's concerns over what providing access in that particular case would mean for future cases).

For example, the Electronic Communications Privacy Act[187] requires (under certain circumstances) not only a warrant, but also that "normal investigative procedures have been tried and have failed" before the government can intercept certain kinds of communications.[188] Such a system could go a long way towards limiting usage to only situations where backdoor access is strictly necessary, as well as assuaging many of the privacy concerns that could arise through attempts to bypass encryption.

C. RESPONDING TO COUNTER-ARGUMENTS: WHY A CASE-BY-CASE BACKDOOR SCHEME MAKES SENSE

The proposed framework outlined in the proceeding Section naturally raises critiques from technology firms, arguing that any device access would weaken encryption for all, as well as from law enforcement, arguing that the limits described mean the proposed framework does not go far enough. This Section examines and responds to these critiques.

1. Even Single-Device Access Would Weaken Device Encryption Overall

From those in favor of strong encryption, a likely response to this proposal is that it makes cellphone encryption weaker overall.[189] This argument is not without merit. As Apple points out, "In the wrong hands, this software . . . would have the potential to unlock any iPhone in someone's physical possession."[190] This response suggests, however, two key limitations that would substantially reduce the risk of this harm occurring. First, the software would have to fall into "the wrong hands." Such access could be minimized by taking the same security measures Apple takes for its in-house testing of new software and applying it to the backdoor software. Additionally, companies could store backdoors offline, ensuring that even if a company is hacked, those hackers will not gain access to the backdoor software.[191] Although offline storage does not eliminate the

187. 18 U.S.C. §§ 2510–2522 (2012).

188. 18 U.S.C. § 2518(3).

189. *See, e.g.*, Danny Yadron, *Security Experts: FBI Asking Apple To Weaken Encryption Is 'Path to Hell,'* THE GUARDIAN (Mar. 1, 2016), https://www.theguardian.com/technology/2016/mar/01/apple-fbi-encryption-fight-security-experts-rsa.

190. Calamur, *supra* note 185.

191. *Cf.* Kurt L. Hudson, *Offline Root Certification Authority (CA)*,

risk of adverse access, it substantially increases the costs, to the point of being prohibitive for all but the most powerful of actors.[192] This would ensure that neither hackers nor even governmental actors would be able to gain access to the backdoor tools.

If this risk is still of great concern, however, companies could independently develop a backdoor each time it is requested, and then destroy all copies of the backdoor tool after its use. Though inefficient, this would ensure that such a tool was never existent for copying by rogue actors. Perhaps the statutory scheme could even factor this in and require the government to foot the cost. In this way, there would be no permanent backdoor for anyone to access, rather it would be ephemeral, existing only for a specific device and only long enough to get the needed information off of that device.

2. Single-Device Access Would Still Permit Many Encrypted Files To Remain Outside the Reach of Law Enforcement

While proponents of strong encryption may worry that permitting single device backdoors would weaken security, law enforcement may argue that such a system does not go far enough. After all, while such a regime would grant access to devices made by companies like Apple and Google, it would not prevent the use of encryption beyond company control. For example, computer users could still download GPG (an open-source version of the PGP software discussed in Part I.A.2) and use encryption not vulnerable to attacks from the privileged position device manufacturers enjoy. Law enforcement may argue that to truly stop encryption from adversely impacting investigations and security, encryption which cannot be made to fit into the framework described above should be made illegal.[193]

MICROSOFT (Sept. 25, 2015), http://social.technet.microsoft.com/wiki/contents/articles/2900.offline-root-certification-authority-ca.aspx (describing proper storage procedures for root certificate authorities, including offline storage).

192. *See, e.g.*, Kim Zetter, *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*, WIRED (Nov. 3, 2014), https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet (describing software that could attack Iranian centrifuges despite those computers not being connected to the Internet).

193. *See supra* Part I.B. No law enforcement agency has actually been making this argument since the 1990s (likely for the reasons discussed in the following sentences), but it is a natural outgrowth of current calls to rein in encryption, and is likely to resurface as part of that debate.

The problem with this argument, however, is that a regulation banning encryption would simply be unenforceable.[194] Any attempt to force open-source software developers to integrate encryption backdoors (regardless of whether they be broad or narrowly tailored) will simply lead to people who truly want government-proof encryption to take the (publically available) source code of those tools, remove the backdoor, and proceed as they did before. Thus, while making unbreakable encryption illegal has intuitive perspective, as a practical matter such a law could never be effectively enacted. To borrow a phrase from the gun lobby, "when backdoor-proof encryption is outlawed, only outlaws will use backdoor-proof encryption."

In summary, although broad encryption backdoors meet with First Amendment obstacles, law enforcement could use multiple other tools that would allow access to a large portion of communications without impinging on the First Amendment. One such tool would be a narrowly tailored access framework, used only in a case-by-case basis. Such a framework would allow access to many communications when law enforcement has justification, while still addressing security concerns that technology firms and privacy advocates may raise.

CONCLUSION

As the Internet continues its pervasive growth into everyday life, encryption is going to be increasingly important, both as a tool to ensure privacy and as a hurdle that law enforcement must overcome in their investigations. Although the access they may provide has obvious appeal, encryption backdoors are not a constitutionally acceptable solution to this hurdle. For all the aid it may provide, broad encryption backdoors are not reconcilable with the First Amendment. Such a requirement would constitute compelled speech, which is permitted only in the presence of a "clear and present danger," not present in all the cases to which the requirement would apply.

Despite this apparent problem, this does not leave law enforcement bereft of tools to obtain encrypted communication information. Using other means of information acquisition, law

194. *See* Andrew Charlesworth, *Munitions, Wiretaps and MP3s: The Changing Interface Between Privacy and Encryption Policy in the Information Society*, *in* THE HISTORY OF INFORMATION SECURITY 771, 782 (Karl de Leeuw & Jan Bergstra eds., 2007) ("[C]ryptographic tools . . . were simply no longer amenable to traditional export oversight and control means. . . . [C]ontaining grey marketers and software pirates . . . was becoming impossible.").

enforcement can still gain access to a wide swath of communications information. By using tools that either do not require any software writing on the part of technology companies, or by limiting requests for backdoors to specific individuals, law enforcement can gain access to a significant portion of the information sought, without crossing the line drawn by the First Amendment.