The Second Amendment and the Struggle Over Cryptography

by ERIC RICE*

Abstract: The United States government and an alliance of Silicon Valley and civil libertarians have been engaged in a struggle over the control of cryptography since the beginning of the information age. The debate has involved various constitutional arguments but has ignored the Second Amendment's right to keep and bear arms. This article argues that in a digital world cryptography qualifies as a weapon, as the U.S. government has (correctly) asserted for decades, and so deserves consideration for Second Amendment protection.

In that analysis, we see that cryptography serves all of the Second Amendment values well. It enables revolution, the defense of minorities, the protection of the sanctity of the home, and the private individual's contribution to the collective defense of the republic. Indeed, it is already the most commonly used weapon in America for self-defense of property and family.

The Second Amendment should be construed to protect cryptography and limit the government's authority to regulate it.

Table of Contents

* J.D., Harvard Law School, 2014; B.A., Columbia University, 2011. Many thanks to Lenore, Bob, Jess, and Isabelle Rice, Natalie Perez, Noah Levin, Alyssa Martin, Edwina Clarke, Matt Tymann, Jonathan Gould, and Michael Parsons for their invaluable help.

I. Introduction

Cryptography, "the art or practice of writing in code or cipher"[1] to keep secrets secret, has existed for millennia.[2] While cryptography is, in one sense just a field of mathematics, it can be implemented in systems for securing information, generally, today, in computer programs.[3] However, for most of history, cryptography's use was restricted almost entirely to governments.[4] That changed abruptly with the advent of public key cryptography in 1976,

1. *Cryptography*, OXFORD ENGLISH DICTIONARY (9th ed. 2016).

2. Jeffrey L. Vagle, *Furtive Encryption: Power Trust and the Constitutional Cost of Collective Surveillance*, 90 IND. L.J. 101, 106 (2015).

3. *See* BRUCE SCHNEIER, DATA & GOLIATH 144 (W.W. NORTON COMPANY) (2015).

4. *See* KENNETH DAM & HERBERT LIN, EDS. CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY, Nat'l Research Council, xiii (1996); Vagle, *supra* note 2, at 199 n.94. Of course, private citizens did occasionally use cryptography to protect their secrets. *See, e.g.*, Vagle, *supra* note 2, at 107 (noting use of cryptography by, *inter alia,* "priests . . . merchants . . . criminals, prisoners, and lovers").

and the subsequent explosion of the internet, especially online banking and commerce.[5] "Since the mid-1990s civilian and commercial use of cryptographic technology has been wide-spread."[6] The loss of this technological monopoly provoked a series of conflicts between the government and the private sector over who should have access to strong cryptography and under what conditions. These conflicts are known as the "Crypto Wars."

Both sides in the Crypto Wars have marshaled various arguments — policy, legal, and constitutional — about whether cryptography should be regulated. Examining the full range of these arguments is beyond the scope of this paper. My goal here is simply to introduce another consideration: the Second Amendment should limit the government's ability to regulate cryptography.

The Second Amendment reads: "A well regulated Militia, being necessary to the security of a free State, the right of the people to keep and bear Arms, shall not be infringed." In *District of Columbia v. Heller*, the Supreme Court held that the Amendment enshrines an individual right to possess arms for self-defense.[7]

In the digital age, self-defense is simply not possible without strong cryptography. Our bank accounts would be open to whatever criminals come along and our every communication would be exposed to government or criminal eavesdropping. Examples of the threats we face are all around us, from electronic bank heists to the Office of Personnel Management losing the personally identifiable information of many U.S. government officials — including those living undercover in hostile environments — to domestic violence survivors being electronically surveilled by their attackers. It is in this context that the National Intelligence Council has called cryptography the "best defense" of personal information from criminals or governments.[8] And so, in the modern world, if the Second Amendment does not protect cryptography, it no longer protects us.

The text of the Second Amendment does not intuitively encompass cryptography. But the word "Arms" is sufficiently ambiguous that it could, and as the world has developed, we should read it to. Indeed, the U.S. government itself has long and explicitly treated cryptography as a weapon,

5. *See* Vagle, *supra* note 2, at 110–115.

6. *Id.* at 115.

7. *District of Columbia v. Heller*, 554 U.S. 570, 573, 128 S. Ct. 2783, 2787 (2008).

8. James Ball, *Secret US Cybersecurity Report: Encryption Vital to Protect Private Data*, THE GUARDIAN, Jan. 15, 2015, *available at* http://www.theguardian.com/us-news/2015/jan/15/-sp-secret-us-cybersecurity-report-encryption-protect-data-cameron-paris-attacks (last accessed Jan. 1, 2016).

which itself should justify consideration of Second Amendment protection for it.

The first part of this paper gives a brief history of the conflict over cryptography in American politics. The second part puts forward the case for considering cryptography an "arm" protected by the Second Amendment. The final section outlines some considerations relevant to applying Second Amendment doctrine to limit government regulation of cryptography.

II. The Crypto Wars

"The fundamental question" at stake in the Crypto Wars "is whether or not governments should legislate against cryptography."[9] On one side, the unusual alliance of big business and civil libertarians says no, arguing that widespread access to strong encryption is key for information security, keeping the government in check, and the success of the American technology industry.[10] On the other side, the law enforcement and national security establishment say yes, arguing that widespread use of powerful cryptography would hamstring government efforts to fight crime, prevent terrorism, and defend the homeland.[11]

A. Crypto Wars v. 1.0

The first iteration of the Crypto Wars was fought primarily on two fronts.[12] One involved export restrictions on cryptography under the U.S. International Traffic in Arms Regulations ("ITAR"). The other involved a federal government plan for the telecommunications industry to adopt encryption systems that allowed for government access to messages.

1. ITAR

Coming out of the Second World War, the United States held a position of world economic dominance that made export controls a plausible tool of foreign policy, and the nascent Cold War seemed a good reason to use them.[13] The

9. SIMON SINGH, THE CODE BOOK: THE SCIENCE OF SECRECY FROM ANCIENT EGYPT TO QUANTUM CRYPTOGRAPHY 303 (1999).

10. *See, e.g.*, *id.* at 303–09; Daniel Moore & Thomas Rid, *Cryptopolitik and the Darknet,* 58 SURVIVAL 7, 8 (2016).

11. SINGH, *supra* note 9, at 303–09.

12. For an exhaustive and thoughtful treatment of the first iteration of the Crypto Wars, see A. Michael Froomkin, *The Metaphor is Key: Cryptography, the Clipper Chip and the Constitution,* 143 U. PA. L. REV. 709 (1995).

13. 22 U.S.C. § 2778(a)(1) (2012); Whitfield Diffie & Susan Landau, *The Export of Cryptography in the 20th Century and the 21st*, *available at* http://privacyink.org/pdf/export_control.pdf (last accessed, Jan. 18, 2016), 4 (also published in THE HISTORY OF INFORMATION SECURITY: A COMPREHENSIVE HANDBOOK, 725 (Karl de Leeuw & Jan Bergstra, eds. 2007)).

Arms Export Control Act gives the President authority — delegated to the State Department — to regulate the export of military technology.[14] The State Department promulgated the International Traffic in Arms Regulations[15] pursuant to this authority.[16] And that regime governs defense specific items, which are listed on the "Munitions List."[17] Items with both commercial and military application — "dual use" items — are regulated by the Secretary of Commerce, pursuant to the Export Administration Regulations ("EAR").[18] Unsurprisingly, the restrictions on the export of "munitions" are far stricter, requiring individually approved export licenses.[19]

In the post-WWII era, the Munitions List included "[c]ryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components or software with the capability of maintaining secrecy or confidentiality of information or information systems."[20] And this was perfectly reasonable, as cryptography was an almost exclusively military tool.[21] However, cryptography remained on the munitions list even as civilian and commercial use of, and need for, cryptography grew with the information revolution in the late twentieth century.[22]

American software companies, in order to send programs including cryptography abroad, needed either an individual license or to request a transfer of jurisdiction to the Commerce Department for their specific product.[23] The licensing process took weeks or months and required the party seeking the license to be able to individually identify the end user.[24] This placed an enormous burden on American companies,[25] and licenses were often denied.[26]

As the American computer industry began to face more serious competition from Europe and Asia, the economic consequences of banning

14. *Id.*

15. 22 C.F.R. §§ 120–30.

16. *See Bernstein v. U.S. Dept. of State,* 922 F. Supp. 1426, 1429 (N.D. Cal. 1996) [*Bernstein I*].

17. DIFFIE & LANDAU, PRIVACY ON THE LINE, 120–23 (2007); 15 C.F.R. §§ 768–99; 50 App. U.S.C. §§ 2401–20.

18. *Id.*

19. DIFFIE & LANDAU, *supra* note 13, at 727.

20. 22 C.F.R. § 121.1 (1996); *see Bernstein I,* 922 F. Supp. at 1429. The regulations did exempt certain cryptographic applications such as the cryptography used in automatic teller machines and some consumer software. *Id.*

21. Diffie & Landau, *supra* note 13, at 4.

22. *Id.*

23. *Id.*

24. *Id.* at 4, 6.

25. *Id.* at 6.

26. *Id.*

the export of cryptography became clear: consumers bought from foreign companies that could provide more secure products.[27] Gradually, political pressure mounted for a change in export policy in order to preserve American competitiveness globally.[28] The first major step towards change came in 1992, when a deal between the National Security Agency ("NSA"), the Department of Commerce, and RSA Data Security allowed for expedited approval of two RSA cryptographic algorithms with relatively short (40 bit) key lengths.[29] Key length is a common measurement of the security of an encryption system (that uses a proven algorithm), as increasing key length dramatically increases the amount of work an attacker must do — and thus time an attacker must spend — to break the encryption.[30]

At the same time, parallel opposition to the ITAR regime began to form, grounded not in concerns about economic competitiveness, but in a libertarian political philosophy. Phil Zimmerman was a programmer and anti-nuclear activist.[31] As Cold War tensions eased, and the risk of nuclear holocaust faded, Zimmerman turned his attention from advocating against nuclear war to advocating for privacy.[32] He believed that the rise of electronic communication was causing a paradigm shift in government surveillance by lowering the cost and effort required, because "email messages are just too easy to intercept and scan for interesting key words. This can be done easily, routinely, automatically, and undetectably on a grand scale."[33] (And time, of course, has proven him right). Cryptography, Zimmerman thought, was the tool that could prevent this "Orwellian" turn.[34] Zimmerman wrote: "[I]n the Information Age, cryptography is about political power, and, in particular, about the power relationship between a government and its people. It is about the right to privacy, freedom of expression, freedom

27. *See id.* at 8.

28. *See id.*

29. *Id.* at 9.

30. *Id.*; SCHNEIER, *supra* note 3, at 144 (2015) ("[A] small change in key length results in an enormous amount of extra work for the attacker. A 64-bit key might take an attacker a day to break. A 65-bit key would take the attacker twice the amount of time to break, or two days. And a 128-bit key — which is at most twice the work to use for encryption — would take the same attacker 264 times longer, or one million billion years to break. (For comparison, Earth is 4.5 billion years old).").

31. SINGH, *supra* note 9, at 295; *see also* Vagle, *supra* note 2, at 113; Diffie & Landau *supra* note 13, at 9; ANDY GREENBERG, THIS MACHINE KILLS SECRETS: HOW WIKILEAKERS, HACKTIVISTS, AND CYPHERPUNKS AIM TO FREE THE WORLD'S INFORMATION, 54 (2012).

32. SINGH, *supra* note 9, at 296.

33. *Id.* at 296.

34. *Id.*

of political association, freedom of the press, freedom from unreasonable search and seizure, freedom to be left alone."[35]

In order to preserve these fundamental political liberties, Zimmerman thought "ordinary people and grassroots political organizations" should have access to "affordable 'military grade' public-key cryptographic technology."[36] To this end, he developed Pretty Good Privacy, or "PGP," an email encryption program.[37] PGP used RSA technology, but keys that were far longer than 40 bits.[38]

In 1991, the U.S. Senate omnibus anticrime bill was put forward.[39] That law included a provision that would have required those producing cryptographic equipment to include "back doors" that would give the government a way to bypass the encryption.[40] Although that provision never became law, Zimmerman feared it would and took a revolutionary step; he published PGP on the Internet, for free.[41]

PGP was soon downloaded abroad, likely putting Zimmerman in violation of ITAR.[42] The U.S. Attorney for the Northern District of California convened a grand jury that spent over a year investigating him, before dropping the case.[43] The U.S. Attorney apparently backed off because of massive public support for Zimmerman, who recalled that "[e]very last article was sympathetic to [him]."[44]

Another possible explanation lies in something that happened shortly before the investigation was dropped: MIT Press published the PGP source code in book format and applied for export permission.[45] When the State Department simply ignored the request, MIT went ahead, published the book, and exported it.[46] This stunt played on MIT's institutional prestige to highlight the First Amendment implications of limiting the export of computer code.

35. *Id.*

36. VAGLE, *supra* note 2, at 114 (quoting PHILLIP ZIMMERMAN, THE OFFICIAL PGP USER'S GUIDE, 5–7 (1995); *see also* SINGH, *supra* note 9, at 296.

37. SINGH, *supra* note 9, at 296.

38. *Id.*

39. *Id.*; VAGLE, *supra* note 2, at 113; GREENBERG, *supra* note 31, at 74.

40. Vagle, *supra* note 2, at 113; SINGH, *supra* note 9, at 295–96; GREENBERG, *supra* note 31, at 74.

41. SINGH, *supra* note 9, at 301; *see also* Vagle, *supra* note 2, at 113; Diffie & Landau, *supra* note 13, at 9.

42. VAGLE, *supra* note 2, at 113; Diffie & Landau, *supra* note 13, at 9.

43. DIFFIE & LANDAU, *supra* note 13, at 9.

44. Quoted in GREENBERG, *supra* note 31, at 86.

45. DIFFIE & LANDAU, *supra* note 13, at 9; GREENBERG, *supra* note 31, at 87.

46. GREENBERG, *supra* note 31, at 86.

Then, in 1996, a Ph.D. candidate in mathematics named Daniel Bernstein, who had developed a new cryptographic protocol, sued the Department of State, in the Northern District of California. Bernstein sought a declaratory judgment stating that including cryptography in the ITAR regime was unconstitutional under the First Amendment and an injunction prohibiting the government from enforcing the regulations against him.[47] The District Court agreed, holding that the licensing scheme was an unconstitutional prior restraint on protected speech.[48]

In December of 1996, just before the District Court's decision, and responding to political pressure from civil libertarians and the tech sector, President Bill Clinton signed Executive Order 13026, which "transferred jurisdiction over the export of non military encryption products to the Department of Commerce."[49] By the end of the month, the Commerce Department had enacted an interim rule regulating the export of encryption under the EAR.[50] Bernstein amended his complaint to challenge the EAR rule.[51] The district court struck down the EAR rule too.[52] The Ninth Circuit affirmed.[53] But that opinion was withdrawn pending an en banc rehearing.[54]

Then the government retreated. In 1998, the Clinton administration relaxed export restrictions on products containing Data Encryption Standard ("DES") technology[55] or using keys of 56 bits or less.[56] Meanwhile, some members of Congress began to push for the so-called Security and Freedom through Encryption ("SAFE") bills, which would have reformed the export regulation scheme.[57] Several such bills had failed when, in 1999, one

47. *Bernstein I*, 922 F. Supp. at 1426.

48. *Bernstein v. U.S. Dept. of State*, 945 F. Supp. 1279, 1286 (N. D. Cal. 1996) [*Bernstein II[* The Government won a similar suit brought by a programmer named Phil Karn, after the State Department denied him permission to export a floppy disk containing the source code for implementing DES. *Karn v. U.S. Dept. of State,* 925 F. Supp. 1, 4 (D.D.C. 1996).

49. *Bernstein v. U.S. Dept. of State,* 974 F. Supp. 1288, 1288 (N. D. Cal. 1997) [*Bernstein III*]; 15 C.F.R Pt. 730 *et seq*.

50. *Bernstein III,* 974 F. Supp. at 1288.

51. *Id.*

52. *Id.*

53. *Bernstein v. U.S. Dept. of State,* 176 F.3d 1132, 1147 (9th Cir. 1999) [*Bernstein IV*] *withdrawn pending en banc reh'g,* 192 F.3d 1308 (9th Cir. 1999).

54. *Bernstein v. U.S. Dept. of State,* 192 F.3d 1308 (9th Cir. 1999). The subsequent changes to the regime and Dep't of Commerce opinions caused Bernstein to lose standing before the rehearing occurred. *Bernstein v. U.S. Dept. of Commerce*, No. C 95-0582, 2004 WL 838163, *1 (N.D. Cal. Apr. 19, 2004).

55. DES was the National Bureau of Standards' favored cryptographic algorithm, developed in 1977. Vagle, *supra* note 2, at 110.

56. DIFFIE & LANDAU, *supra* note 13, at 12.

57. *Id.*

survived its committee hearings and was on the cusp of debate in the Senate.[58] At this point, (likely because Vice-President Al Gore saw Silicon Valley as an important constituency for his upcoming presidential campaign), the executive branch made a major concession and agreed that key length would no longer be a factor in determining whether cryptographic technology could be exported.[59]

The old export system was replaced with a regime that strives to make a meaningful distinction between civilian or "retail" cryptography and cryptography specialized for military use.[60] "Retail" cryptography products must be submitted for a one-time review and if the company does not hear anything within 30 days, it is free to sell it.[61] Open source software is entirely exempted.[62] While some military specific cryptographic technologies remain on the munitions list,[63] this was a "virtually complete capitulation."[64]

2. The Clipper Chip

The second front of the original Crypto Wars became "an epic battle that would preoccupy a generation of cryptographers."[65] This second front grew out of the ITAR fight when the administration promised relaxed export control for companies that agreed to put backdoors into their technology.[66] In 1993, the Clinton administration attempted to replace the then national standard cryptographic algorithm, 50-bit DES, with a so called "key escrow" system, a new 80-bit algorithm that provided the government with a "backdoor," a technical means to access data without first obtaining the password: the Escrowed Encryption System.[67] This was "the infamous Clipper system."[68]

58. *Id.* at 14.

59. *Id.*

60. *Id.*

61. *Id.* at 14–15.

62. *Id.* at 15–16.

63. *See* 22 C.F.R. § 121.1 Category XII (b)(1).

64. DIFFIE & LANDAU, *supra* note 13, at 16.

65. Matt Blaze, *Key Escrow from a Safe Distance: Looking Back at the Clipper Chip*, in ACSAC' 11 PROCEEDINGS OF THE 27TH ANNUAL COMPUTER SECURITY APPLICATIONS CONFERENCE, at 317.

66. *Id.* at 1; DIFFIE & LANDAU, *supra* note 13, at 10 and n.9.

67. DIFFIE & LANDAU, *supra* note 13, at 10 and n.9; U.S. Dep't of Commerce & Nat'l Inst. Standards & Tech., *Approval of Federal Information Processing Standards Publication 185, Escrowed Encryption Standard,* 27 Fed. Reg. 59 (Feb. 9, 1994).

68. DIFFIE & LANDAU, *supra* note 13, at 10 and n.9. Clipper was intended for telephonic communication; "Capstone" was a similar system intended for computer communication. Singh, *supra* note 9, at 310; Diffie & Landau, *supra* note 17, 239–40.

At the time, most encryption technology was hardware based — the cryptographic algorithms were physically built into computer chips rather than implemented by software code — and the Clipper chip was meant to be easily substituted for the chips in existing secure telephone hardware.[69] Clipper used a new algorithm, named "Skipjack," developed by the NSA and highly classified, but presumably strong.[70]

However, Clipper, of course, had a backdoor. Clipper operated by first transmitting a so-called "Law Enforcement Access Field" ("LEAF") at the beginning of every message.[71] The LEAF contained the session key that was used to encrypt the message, and was itself encrypted with a different key that the government had access to.[72] Thus, in order to read a message, the government simply had to use its key to decrypt the LEAF, and then use the session key contained therein to decrypt the message.[73]

Policy makers thought this an ideal solution that balanced the public's demand for secure communication with the government's desire for access to those communications.[74] They never succeeded, however, in selling the skeptical public and tech industry on it.[75] There were several reasons for this. First, because Skipjack was classified, it was never subject to the sort of public stress-testing vital to ensuring the security of a cipher.[76] Second, Clipper was introduced at a time when hardware encryption was being rapidly replaced by cheaper software encryption.[77] Third, when export restrictions were lifted, the government lost its most important source of leverage for incentivizing its adoption.[78] Fourth, there were serious problems with the way the back door functioned: when Matt Blaze, a researcher at AT&T Bell Labs, published a paper outlining ways in which the LEAF system could be circumvented, his findings were published on the

69. *See* BLAZE, *supra* note 65, at 319.

70. *Id.* at 317.

71. *Id.* at 318.

72. *Id.*

73. *Id.*

74. *Id.*

75. *See, e.g.*, LAWRENCE LESSIG, CODE 2.0, 52 (2006).

76. Cryptographers are in near universal agreement that only systems which depend solely on keeping the encryption key secret are trustworthy. *See* BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY (2d ed.), 7 (1996); *see also* Bruce Schneier, *Secrecy, Security, and Obscurity,* CRYPTOGRAM, May 15, 2002, *available at* https://www.schneier.com/crypto-gram/archives/2002/0515.html (last accessed June 1, 2015).

77. BLAZE, *supra* note 65, at 321.

78. *Id.*

front page of *The New York Times*, above the fold.[79] Fifth, the key escrow feature created security problems that potentially endangered the secrecy of the underlying message.[80] Finally, many worried that adoption of Clipper would hurt American products in overseas markets.[81]

Over the course of the next decade, the government tried unsuccessfully to push the adoption of various forms of similar systems.[82] These failed for the same reasons. Like ITAR, the Clipper chip and its progeny were simply politically unfeasible.[83] Key escrow became an issue that stoked strong reactions from, and an unlikely alliance between, the far left and the far right: the ACLU and Rush Limbaugh criticized the plan with equal vigor.[84] According to one CNN poll, 80 percent of Americans opposed the Clipper plan.[85] In the face of this united front, the government backed off.

B. Crypto Wars v. 2.0

After the overhaul of the export regime and the defeat of Clipper, the civil-libertarian-Silicon Valley alliance believed it had won the Crypto Wars.[86] But in 2014, major technology companies made the decision to bring encryption to the masses as never before, and the war was back on.

1. Apple and Google Fire on Fort Meade

In the fall of 2014, Apple and Google increased the cryptographic protections they offered to smartphone users. Apple was suffering from negative publicity due to the theft of nude photos from celebrities' Apple

79. *Id.* at 318–320; GREENBERG, *supra* note 31, at 86. Matt Blaze, *Protocol Failure in Escrowed Encryption Standard, available at* http://www.crypto.com/papers/eesproto.pdf (last accessed Aug. 4, 2016). The flaws Blaze discovered did not in fact allow the attacker to access the plain-text of a message but rather allowed for a user to bypass the LEAF mechanism altogether. Matt Greene, *A History of Backdoors*, A FEW THOUGHTS ON CRYPTOGRAPHIC ENGINEERING, July 20, 2015, *available at* http://blog.cryptographyengineering.com/2015/07/a-history-of-backdoors.html (last accessed, Jan. 18, 2016).

80. *Id.* at 321.

81. Steven Levy, *The Battle of the Clipper Chip*, N.Y. TIMES MAG., June 12, 1994, *available at* http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html (last accessed Apr. 18, 2015).

82. BLAZE, *supra* note 65, at 321.

83. LEVY, *supra* note 81, at 1.

84. *Id.*

85. GREENBERG, *supra* note 31, at 86.

86. Electronic Frontier Foundation, *The Crypto Wars: Governments Working to Undermine Encryption, available at* https://www.eff.org/document/crypto-wars-governments-working-undermine-encryption (last accessed Apr. 19, 2015); We now know that behind the scenes, the NSA was still working to weaken the cryptographic protocols advanced by the National Institute of Standards and Technology to be the standard protocols across the internet. SHANE HARRIS, @WAR THE RISE OF THE MILITARY-INTERNET COMPLEX 88–93 (HOUGHTON MIFFLIN HARCOURT) (2014).

accounts, and both companies were catering to consumer attitudes towards privacy that were assumed to have shifted dramatically following the Snowden revelations about the scope of NSA surveillance.[87]

First, Apple announced that the new iPhone operating system would automatically encrypt the contents of iPhones in such a way that the company could not access them.[88] Thus Apple could not provide information on iPhones to law enforcement, even pursuant to a warrant.[89] Prior to this change, Apple had a policy of unlocking phones pursuant to valid court orders.[90]

Google immediately followed suit. Although Google had apparently never kept the encryption keys for Android phones,[91] it began encrypting the phones running the Android operating system by default, rather than forcing users to actively choose to encrypt them.[92]

2. The Empire Strikes Back

While privacy advocates lauded these decisions, law enforcement officials rushed to condemn them. FBI Director James Comey was one of the earliest and most vehement critics. Comey claimed that he feared a time when an investigation would hinge on accessing the contents of a smart phone and "people with tears in their eyes [would] look at [him] and say, 'What do you mean you can't?'"[93] Not to be outdone in the rhetoric department, Chicago's chief of detectives proclaimed: "Apple will become

87. *See, e.g.*, Craig Timberg, *Newest Androids will join iPhones in offering default encryption, blocking police*, WASH. POST, Sept. 18, 2014, *available at* http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/ (last accessed Apr.15, 2015).

88. Craig Timberg, *Apple Will no Longer Unlock Most iPhones, iPads for Police, Even With Search Warrants* WASH. POST, Sept. 18, 2014, *available at* http://www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html (last accessed Apr.14, 2015).

89. *Id.*

90. *Id.* It is worth noting here that it is not clear whether Apple actually retained keys that allowed it to access the encrypted information on the phone or if so much of the information was unencrypted that it did not matter. *See* Matthew Green, *Why can't Apple decrypt your iPhone,* A FEW THOUGHTS ON CRYPTOGRAPHIC ENGINEERING, Oct. 4, 2014, *available at* http://blog.cryptographyengineering.com/2014/10/why-cant-apple-decrypt-your-iphone.html (last accessed Apr. 22, 2015).

91. Ron Amadeo, *Android L will have device encryption by default*, ARSTECHNICA, *available at* http://arstechnica.com/gadgets/2014/09/android-l-will-have-device-encryption-on-by-default/ (last accessed Apr. 15, 2015).

92. TIMBERG, *supra* note 87.

93. Ken Dilanian, *FBI chief: Apple, Google phone encryption perilous*, ASSOCIATED PRESS, Sept. 25, 2014, *available at* http://bigstory.ap.org/article/420160593748455390db7aeaf0abafdc/fbi-chief-new-phone-encryption-could-cost-lives (last accessed Apr. 15, 2015).

the phone of choice for the pedophile . . . . The average pedophile at this point is probably thinking, 'I've got to get an Apple phone.'"[94]

In remarks at the Brookings Institute, Director Comey articulated his concern over "going dark," a phenomenon he described thusly: "Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority. We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so."[95] Comey cautioned that "encryption threatens to lead all of us to a very dark place," depicting a world in which kidnappers and terrorists could successfully hide behind the encryption on their phones.[96]

Comey also anticipated the argument that even when phones are encrypted, the government has sufficient tools to investigate crimes. He explained that metadata (such as telephone records) — which is generally unaffected by encryption — does not provide a communications content and that brute-force attacks on passwords are difficult even with super-computers.[97] Acknowledging that the information from devices that are backed up to "cloud" storage is generally encrypted with keys a company, rather than an individual holds, he argued that criminals are unlikely to back-up their devices. Lastly, Comey argued that it is unlikely law enforcement could compel defendants to decrypt their phones (presumably meaning consistent with the Fifth Amendment) and that in any event, contempt punishments are inadequate to effectively compel compliance with court orders.[98]

Other government officials expressed similar concerns, including Attorney General Holder,[99] NSA Director Admiral Rogers,[100] UK Prime

94. *Id.*

95. James Comey, *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course*, Oct. 16, 2014, *available at* http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course (last accessed Apr. 15, 2015).

96. *Id.*

97. *Id.*

98. *Id.*

99. Craig Timberg, *Holder urges tech companies to leave device backdoors open for police,* WASH. POST, Sept. 20, 2014, *available at* http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/30/holder-urges-tech-companies-to-leave-device-backdoors-open-for-police/ (last accessed Apr.15, 2015).

100. John Reed, *Transcript: NSA Director Mike Rogers v. Yahoo! on Encryption Back Doors*, JUST SECURITY, Feb. 23, 2015, *available at* http://justsecurity.org/20304/transcript-nsa-director-mike-rogers-vs-yahoo-encryption-doors/ (last accessed Apr. 15, 2015).

Minister Cameron,[101] and President Obama.[102] The law enforcement establishment was again pushing for strict regulations on cryptography and it seemed that a full reprise of the crypto wars was underway. In general, these policy makers advocated for requiring companies to include "backdoors," like the Clipper Chip.[103]

3. An Uneasy Truce

Over the course of about a year a debate over backdoors raged between law enforcement on one side and the tech industry and civil libertarians on the other. However, in thepost-Snowden world, it seemed that those in favor of strong encryption were winning the day in the court of public opinion.[104] In the fall of 2015, a leaked National Security Council white paper showed that the administration had apparently decided not to seek legislation or otherwise compel backdoors in cryptography.[105] The war had apparently ended as suddenly as it had started.

As one law enforcement official stated: "People are still not persuaded this is a problem. People think we have not made the case. We do not have the perfect example where you have the dead child or a terrorist act to point to, and that's what people seem to claim you have to have."[106] But that statement itself contains the seeds of another war: If they got such a case, the debate would be entirely different. As another official wrote, "the legislative environment is very hostile today . . . [but] it could turn in the event of a terrorist attack or criminal event where strong encryption can be shown to have hindered law enforcement."[107]

101. Nicholas Watt, et al., *David Cameron pledges anti-terror law for internet after Paris attacks*, THE GUARDIAN, *available at* http://www.theguardian.com/uk-news/2015/jan/12/david-cameron-pledges-anti-terror-law-internet-paris-attacks-nick-clegg (last accessed Apr. 15, 2015).

102. Julian Hattem, *Obama backs calls for tech backdoors*, THE HILL, Jan. 16, 2015, *available at* http://thehill.com/policy/technology/229787-obama-backs-call-for-tech-backdoors (last accessed Apr. 15, 2015).

103. TIMBERG, *supra* note 99; Comey, *supra* note 95; Reed, *supra* note 100; Watt, et al. *supra* note 101.

104. Ellen Nakashima & Andrea Peterson, *Obama faces growing momentum to support widespread encryption*, WASH. POST, Sept. 16, 2015, *available at* https://www.washingtonpost.com/world/national-security/tech-trade-agencies-push-to-disavow-law-requiring-decryption-of-phones/2015/09/16/1fca5f72-5adf-11e5-b38e-06883aacba64_story.html (last accessed Nov. 18, 2015).

105. *Read the NSC Draft Options Paper on Strategic Approaches to Encryption*, WASH. POST, http://apps.washingtonpost.com/g/documents/national/read-the-nsc-draft-options-paper-on-strategic-approaches-to-encryption/1742/ (last accessed Nov. 18, 2015).

106. Nakashima & Peterson, *supra* note 104.

107. *Id.*

Within days of the November 2015 terrorist attack on Paris, the debate was rekindled, as reports surfaced that the attackers had used encrypted communications to coordinate their attacks.[108] And it only intensified after the attacks in San Bernadino, California.[109] In January of 2016, state legislators in New York and California introduced bills that would ban the retail sale of smartphones with full disk encryption.[110] In February of 2016, Apple and the Department of Justice began a court battle over whether a court could force Apple to create a new operating system to load onto the security of the San Bernadino gunman's iPhone in order to disable some of the security features. And in April of2016 the Chairman and Vice Chairman of the Senate Select Committee on Intelligence introduced the "Compliance with Court Orders Act of 2016."[111] That Bill would have required companies that received a court order compelling it turn over certain data to "provide such information or data . . . in an intelligible format" or "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."[112] While the bill would have left the engineering details of compliance to individual companies, it would have effectively mandated backdoored systems. That bill met with vitriolic opposition, and was dead in the water by May of 2016.[113]

In short, this conflict is unlikely to end definitively anytime soon. And it is in that context that this paper seeks to add another wrinkle to the discussion.

108. *See e.g.*, David E. Sanger & Nicole Perlroth, *Encrypted Messaging Apps Face New Scrutiny Over Possible Role in Paris Attacks,* N.Y. TIMES, Nov. 16, 2015, *available at* http://www.nytimes.com/2015/11/17/world/europe/encrypted-messaging-apps-face-new-scrutiny-over-possible-role-in-paris-attacks.html?_r=0 (last accessed Nov. 18, 2015).

109. *See e.g.*, *Feds, Silicon Valley headed for 'collision' over encryption issue, post San Bernardino, wave of terror attacks*, FOX NEWS, Dec. 13, 2015, *available at* http://www.foxnews.com/politics/2015/12/13/feds-silicon-valley-headed-for-collision-over-encryption-issue-post-san-bernardino-wave-terror-attacks.html (last accessed Jan. 18, 2016).

110. Andy Greenberg, *Proposed State Bans on Phone Encryption Make No Sense,* WIRED, Jan. 27, 2016, *available at* http://www.wired.com/2016/01/proposed-state-bans-on-phone-encryption-make-zero-sense/ (last accessed Jan. 28, 2016).

111. *Intelligence Committee Leaders Release Discussion Draft of Encryption Bill* (Apr. 13, 2016), http://www.feinstein.senate.gov/public/index.cfm/2016/4/intelligence-committee-leaders-release-discussion-draft-of-encryption-legislation (last accessed May 31, 2016).

112. Compliance with Court Orders Act of 2016 (discussion draft), 114th Cong. (2nd Sess. 2016), *available at* http://www.burr.senate.gov/imo/media/doc/BAG16460.pdf (last accessed May 31, 2016).

113. Dustin Volz, et al., *Push for Encryption Law Falters Despite Apple Case Spotlight*, REUTERS, May 27, 2016, http://www.reuters.com/article/us-usa-encryption-legislation-idUSKCN0YI0EM (last accessed May 31, 2016).

III. Priming the Second Amendment

The Second Amendment states: "A well regulated Militia, being necessary to the security of a free State, the right of the people to keep and bear Arms, shall not be infringed."[114] The text is divided into two parts: the prefatory clause ("A . . . free State,") and the operative clause ("the right . . . infringed").[115]

For most of American history, the Second Amendment was a backwater of political and constitutional thought.[116] It was the subject of only the occasional decision and little scholarship. The Amendment did enjoy some time in the limelight as a centerpiece of Charles Sumner's speech, "The Crime Against Kansas,"[117] and during reconstruction.[118] Similarly, in the 1960s, Black nationalists, including Malcom X and the Black Panthers, breathed some life into the Second Amendment.[119]

Nonetheless, by the 1980s, "the Second Amendment languished in relative obscurity" and had been called "obsolete, defunct, and an unused provision, with no meaning for the twentieth century," let alone the twenty-first.[120] But then, in the 1980s and 1990s, the National Rifle Association and the modern gun rights movement dusted off the Second Amendment and shoved it into the middle of a modern debate.[121] That political shift coincided with a flood of Second Amendment scholarship.[122] While much of this was funded by the NRA,[123] respected liberal scholars — including Akhil Amar[124]

114. U.S. CONST. amend. II.

115. *See* Heller, 554 U.S. at 577.

116. *See* Stuart Banner, *The Second Amendment, So Far,* 117 HARV. L. REV. 898, 898 (2004) (book review).

117. The Crime Against Kansas, May 19–20, 1856, in AMERICAN SPEECHES: POLITICAL ORATORY FROM THE REVOLUTION TO THE CIVIL WAR 553, 606–607 (T. Widmer ed. 2006); *see also Heller*, 554 U.S. at 609.

118. *See* McDonald v. City of Chicago, 561 U.S. 742, 770–77 (2010); ADAM WINKLER, GUNFIGHT 142 (W. W. Norton & Co. 2013); Akhil Reed Amar, *The Second Amendment: A Case Study in Constitutional Interpretation*, 2001 UTAH L. REV. 889, 899 (2001).

119. Jill Lepore, *Battleground America,* THE NEW YORKER, Apr. 23, 2012, *available at* http://www.newyorker.com/magazine/2012/04/23/battleground-america; ADAM WINKLER, GUNFIGHT, 230–47 (W. W. Norton & Co. 2013).

120. BANNER, *supra* note 116, at 898 (quoting Robert E. Shalhope, *The Ideological Origins of the Second Amendment,* 69. J. AM. HIST. 599, 599 (1982) (internal quotations omitted)); Lepore, *supra* note 119 ("In the two centuries following the adoption of the Bill of Rights, in 1791, no amendment received less attention than the Second, except the Third.").

121. *See* BANNER, *supra* note 116, at 901; Lepore, *supra* note 119.

122. *See* BANNER, *supra* note 116, at 901; Lepore, *supra* note 119; MICHAEL WALDMAN, THE SECOND AMENDMENT: A BIOGRAPHY, 97–98 (2014).

123. WALDMAN, *supra* note 122, 97–98; Jill Lepore, *supra* note 119.

124. Akhil Reed Amar, *Second Thoughts,* THE NEW REPUBLIC, July 12, 1999.

and Sanford Levinson[125] — pitched in as well.[126] Thus, by the beginning of the new millennium, the Second Amendment had "become part of the mainstream discourse about the Constitution."[127]

In this period, debate about the Amendment focused on the significance of the prefatory clause and whether the Amendment protected an individual right or a collective right.[128] One school of thought, generally associated with the political right, was that the prefatory clause only announced a purpose and the Amendment applied to ordinary citizens and the arms they own for self-defense, hunting, etc.[129] The opposite view, generally associated with the political left, was that the prefatory clause constrained the right, and the Amendment only restricted the federal government's ability to interfere with State militias.[130] Most of the federal circuits took a middle ground approach — the so called "sophisticated collective right" or "quasi-collective right" model — ruling that the right belonged to individuals, but only individuals connected to some sort of state militia and only protected weapons suitable for use in such a militia.[131] Although formally a compromise, this approach skewed towards a statist view.[132] Then, in 2001, the Fifth Circuit bucked the trend and became the first United States Court of Appeals to endorse the individual rights view of the Second Amendment, with its opinion in *United States v. Emerson*.[133] In 2007, the D.C. Circuit followed suit.[134]

125. Sanford Levinson, *The Embarrassing Second Amendment,* 99 YALE L.J. 637 (1989).

126. WALDMAN, *supra* note 122, 99.

127. BANNER, *supra* note 116, at 899.

128. *Id.* at 902–03.

129. *Id.* at 903.

130. *Id.*

131. *Id.* (citing Gillespie v. City of Indianapolis, 185 F.3d 693, 710–11 (7th Cir. 1999); United States v. Wright, 117 F.3d 1265, 1274 & n.18 (11th Cir. 1997); United States v. Rybar, 103 F.3d 273, 286 (3d Cir. 1996); Love v. Pepersack, 47 F.3d 120, 124 (4th Cir. 1995); United States v. Hale, 978 F.2d 1016, 1019–20 (8th Cir. 1992); United States v. Oakes, 564 F.2d 384, 387 (10th Cir. 1977); Cases v. United States, 131 F.2d 916, 922 (1st Cir. 1942)); *see also* United States v. Emerson, 270 F.3d 203, 219 (5th Cir. 2001)); Cass R. Sunstein, *Second Amendment Minimalism: Heller as Griswold*, 122 HARV. L. REV. 246, 252 (2008) ("Between 1942 and 2001 lower courts had been virtually unanimous in rejecting the view that the Second Amendment creates an individual right to use guns for nonmilitary purposes"); Steven G. Bradbury, et al., *Whether the Second Amendment Secures an Individual Right,* 28 OP. O.L.C. 126, 127 (2004).

132. Emerson, 270 F.3d at 219.

133. *Id.* For a clear, exhaustive and compelling account of the argument for the individual rights view, see Bradbury, *supra* note 131.

134. *See Parker v. Dist. of Columbia*, 478 F.3d 370, 380, (D.C. Cir. 2007).

In 2008, the Supreme Court weighed in, with its enormously controversial[135] decision in *District of Columbia v. Heller*.[136] *Heller* struck down the District of Columbia's strict gun control laws, and settled the personal versus collective right debate by holding that the Second Amendment guarantees an individual right to keep and bear arms for the purpose of self-defense in the home.[137] However, the Court was careful to indicate that there are limits on this right, clarifying that "certain longstanding" gun regulations are constitutionally permissible[138] and that the right extends only to "'arms in common use at the time' for lawful purposes like self-defense."[139] Notably, however, *Heller* declined to articulate a standard of review to be used in Second Amendment cases, reasoning that the D.C. law at issue was so draconian — because it "bann[ed] from the home the most preferred firearm in the nation to keep and use for protection of one's home and family" — as to be unconstitutional under any standard.[140] Two years later, the Court decided *McDonald v. City of Chicago*, holding that the Fourteenth Amendment incorporated the Second Amendment against state and local governments.[141]

Heller and *McDonald* set off an explosion of Second Amendment litigation.[142] Thus, the lower courts have scrambled to put together "the doctrinal plumbing" necessary to address these cases.[143] That scramble has produced a widely accepted two-step process for analyzing Second Amendment claims.[144] A court first determines "whether the challenged law

135. *See, e.g.*, J. Harvie Wilkinson III, *Of Guns, Abortions, and the Unraveling Rule of Law,* 95 VA. L. REV. 253 (2009); Richard A. Posner, *In Defense of Looseness: The Supreme Court and Gun Control,* THE NEW REPUBLIC, Aug. 27, 2008, at 32.

136. *Heller*, 554 U.S. 570 (2008).

137. *Id.* at 592.

138. *Id.* at 626–27.

139. *Id.* at 624 (quoting *United States v. Miller,* 307 U.S. 174, 179 (1939)).

140. *Id.* at 628–29 (internal quotation marks omitted).

141. 561 U.S. 742, 791 (2010); *see also id.* at 858 (Thomas, J., concurring in part and concurring in the judgment) (relying on the Privileges and Immunities Clause, rather than the Due Process Clause).

142. *See, e.g.*, *Peruta v. Cnty. of San Diego,* 742 F.3d 1144, 1180 (9th Cir. 2014) (Thomas, J., dissenting).

143. Lawrence Rosenthal, *Second Amendment Plumbing After McDonald: Exploring the Contradiction in the Second Amendment,* 105 NW. U. L. REV. 437 (2011) (colloquy debate with Joyce Lee Malcolm).

144. *See* Fyock v. Sunnyvale, 779 F.3d 991, 996 (9th Cir. 2015) ("To evaluate post-*Heller* Second Amendment claims, the Ninth Circuit, consistent with the majority of our sister circuits, employs a two-prong test."); *see also,* Heller v. District of Columbia*,* 670 F.3d 1244, 1251–58 (D.C. Cir. 2011)[*Heller II*]; United States v. Marzzarella*,* 614 F.3d 85, 89 (3d Cir. 2010); United States v. Chester*,* 628 F.3d. 673, 680 (4th Cir. 2010); *Ezell v. City of Chicago*, 651 F.3d 684, 701–704 (7th Cir. 2011); United States v. Reese*,* 627 F.3d 792, 800–05 (10th Cir. 2010); *but see*

burdens conduct protected by the Second Amendment."[145] If it does not, the inquiry is at an end. If it does, the court next decides upon and applies "an appropriate level of scrutiny."[146]

We turn now to discuss the obvious threshold question regarding how regulations on cryptography should be treated at the first step.

IV. Is Cryptography an Arm?

In order for the Second Amendment to apply, cryptography must be an "arm." That it may be seems counterintuitive. But this is only because of how dramatically recent technological developments have changed the character of security and the sorts of tools we need to defend ourselves. Upon examination of the purposes of the Second Amendment in light of those modern developments, it becomes clear that cryptography should be considered an arm.

A. The Text and *Heller*

Of course, the first question we must ask is whether this interpretation is consistent with the text of the Constitution. That is, can the word "Arms" plausibly be read to encompass cryptography?

Because most Second Amendment litigation has been focused on firearms, federal courts have had remarkably little occasion to address the question of what is an "arm."[147] *Heller* explained that the meaning of "Arms" today is no different from the 18th century meaning.[148] One 18th century dictionary, quoted in *Heller*, defined "arms" as "weapons of offence, or armor of defense;"[149] another as "any thing that a man wears for his defence, or takes into his hands, or useth in wrath to cast at or strike another."[150]

Paying attention to the term "weapon" is helpful for determining whether cryptography can be considered an "arm." *Heller* uses the terms

Friedman v. City of Highland Park, 784 F.3d 406, 410 (7th Cir. 2015) ("[W]e think it better to ask whether a regulation bans weapons that were common at the time of ratification or those that have some reasonable relationship to the preservation or efficiency of a well regulated militia, and whether law-abiding citizens retain adequate means of self-defense.") (internal quotation marks and citations omitted)).

145. *United States v Chovan*, 735 F.3d 1127, 1136 (9th Cir. 2013).

146. *See id.* This can be framed as a three-step test, *see Friedman,* 784 F.3d at 415 (Manion, J., dissenting), but whether the test is broken into two or three steps is largely irrelevant.

147. Two key state court cases to address the question are City of Seattle v. Evans, 366 P.3d 906, and State v. DeCiccio, 105 A.3d 165 (Conn. 2014).

148. *Heller,* 554 U.S. at 581.

149. *Id.* (*quoting* 1 DICTIONARY OF THE ENGLISH LANGUAGE, 106 (Samuel Johnson, ed.) (4th ed.) (reprinted 1978)).

150. *Id.* (quoting 1 A NEW AND COMPLETE LAW DICTIONARY (Timothy Cunningham, ed. 1771).

"arm" and "weapon" interchangeably through much of the opinion and states that "the most natural reading of 'keep Arms' in the Second Amendment is to 'have weapons.'"[151] *Heller* cites Justice Ginsberg's opinion in *Muscarello v. United States*[152] for the proposition that to "bear arms" means to carry a "weapon" "for the purpose of . . . being armed and ready for offensive and defensive action in case of conflict with another person."[153] We might infer from this that a weapon, or arm, is something that one carries "in case of conflict with another person."[154] Similarly, Webster's defines "weapon" as: "An instrument of offensive or defensive combat" or "a means of contending against another."[155] Ultimately, "arms" or "weapons" include a wide range of instruments that are used — offensively or defensively — in conflict or combat with another person.

This understanding has guided the state supreme courts that have addressed questions of what is an "arm." The Connecticut Supreme Court, in deciding that dirk knives are "arms" for the purposes of the Second Amendment, focused largely on the distinction between utilitarian tools and tools designed for combat.[156] The Court engaged in a lengthy analysis of the history of knives in general, and dirks in particular, beginning with the knives of the Roman legionnaires, through the dirks of the Scottish highlands, to the Ka-Bar fighting knives issued to Marines in Vietnam.[157] The Washington Supreme Court engaged in a similar analysis in determining that paring knives are not arms.[158] That Court held that paring knives are no different from any every day object "which might be effectively wielded for protection or attack," such as rolling pins, frying pans, and candlesticks.[159] Because the paring knife was not designed for conflict, the Washington Supreme Court held that it was not an "arm."[160]

Unlike paring knives, cryptography was designed for conflict. Indeed, it is only useful in case of conflict with another person. While guns may be

151. *Id.* at 582.

152. 524 U.S. 125, 131 (1998).

153. *Heller,* 554 U.S. at 584 (quoting *Muscarello*, 524 U.S. at 131).

154. *Id.* (quoting *Muscarello*, 524 U.S. at 131).

155. WEBSTER'S II NEW RIVERSIDE UNIVERSITY DICTIONARY, 1307 (1988) (defining "weapon" as "[a]n offensive or defensive combat instrument" or "[a] means employed to overcome, persuade, or get the better of another"); *see also* THE AMERICAN HERITAGE DICTIONARY, 1369 (1991) (defining "weapon" as "[a]n instrument used in offensive or defensive combat" or "[a] means employed to disarm, persuade, or get the better of another").

156. *DeCiccio*, 105 A.3d 175.

157. *Id.* at 192–193.

158. *See Evans*, 366 P.3d 906, 906.

159. *See id.* at 872.

160. *Id.*

used to hunt, and axes to log — even dirks are useful for cutting food — cryptography is only useful when there are other people seeking to steal your secrets, impersonate you, or otherwise harm you. Gary Wills wrote, "[o]ne does not bear arms against a rabbit."[161] Ditto cryptography.

Cryptography's centrality to conflict — and the centrality of conflict to cryptography — explains why the use of cryptography was limited to soldiers, spies, and diplomats for most of history.[162] Indeed, if we think back to the ITAR debate during the first iteration of the Crypto Wars, the United States government itself considered cryptography an "arm" for much of the twentieth century.[163] Cryptography lived on the "munitions list," rather than the dual use list, precisely because it was almost exclusively useful for military conflict until recently.[164] And when we consider the role cryptography played in the Second World War[165] and the rhetoric of the Crypto Wars, the idea that cryptography is an arm begins to seem plausible.

However, there are two key objections to overcome. The first is that cryptography is not a physical object like a rifle. And it is true that no case has extended the Second Amendment to protect intangible things. Looking at those 18th century definitions, "takes into his hands" may imply physical instruments. But "useth" is much broader, and nothing about the definitions of the terms "arm," "weapon," or "thing" inherently limits them to physical items — even if most are physical items — as opposed to concepts or ideas.[166] More importantly, in the digital age, "arms" can be no more limited to analog technology than can the "speech" protected by the First Amendment or "searches," that the Fourth Amendment protects against. Today, the term "speech" includes video games,[167] and virtual child pornography.[168] "Searches" include thermal imaging of a dwelling taken n

161. Garry Wills, *To Keep and Bear Arms,* N.Y. REV. BOOKS, Sept. 21, 1995

162. *See, e.g.*, DAM & LIN, *supra* note 4, at xiii; Vagle, *supra* note 2, at 199 n. 94.

163. *See* Diffie & Landau, *supra* note 13, at 5–6.

164. *See id.*

165. *See, e.g.*, DIFFIE & LANDAU, *supra* note 17, at 6–7, MAX HASTINGS, THE SECRET WAR: SPIES, CIPHERS, AND GUERRILLAS 1939–1945, 83, 157, 394–95, 403, 407–08, 545, 548–49 (2016).

166. *See, e.g.*, *Arms*, OXFORD ENGLISH DICTIONARY, *available at* http://www.oed.com/view/Entry/10809?isAdvanced=false&result=3&rskey=LavZO4& (last accessed Jan. 26, 2016); *Arm, n.2*, WEBSTER'S II NEW RIVERSIDE UNIVERSITY DICTIONARY (1984); *Weapon, n.*, OXFORD ENGLISH DICTIONARY, *available at* http://www.oed.com/view/Entry/226597?rskey=I91pBR&result=1&isAdvanced=false#eid (last accessed July 19, 2016); *Thing, n.1*, OXFORD ENGLISH DICTIONARY, *available at* http://www.oed.com/view/Entry/200786?rskey=Ah9QTB&result=1&isAdvanced=false#eid (last accessed July 19, 2016).

167. *See* Brown v. Entertainment Merchants Ass'n, 564 U.S. 786, 790 (2011).

168. *See* Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002).

from the street,[169] and the attachment of a GPS tracking device to a car.[170] Like those terms, "arms" must be read in light of the digital age we now live in, an age in which the United States military has an entire command devoted to electronic warfare,[171] and electronic weapons have been used to destroy Iranian centrifuges,[172] and "cyber" operations figure prominently in American plans for wars with world powers.[173] Thus, despite cryptography being intangible this should pose no obstacle to it being considered an arm.

Another possible objection is that the term "arms" most intuitively encompasses only offensive tools. However, definitions that *Heller* relies on clearly indicate that defensive tools are just as much arms as offensive tools. Those definitions explicitly include "armor of defense"[174] and "any thing that a man wears for his defence."[175] For this reason Eugene Volohk has suggested,[176] and several district courts have assumed without deciding,[177] that body armor is an "arm." Although one district court has held that body armor is not an "Arm,"[178] that conclusion is in obvious tension with *Heller*'s language, which makes clear that the term "arms" is not limited to offensive tools.[179]

Thus, as a purely textual matter, "arms" is at least an ambiguous term that can be interpreted to encompass cryptography. We should therefore look to the Second Amendment's history and purpose to resolve the ambiguity.[180]

169. *See* Kyllo v. U.S., 533 U.S. 27, 34–35 (2011).

170. *See* United States v. Jones, 132 S.Ct. 945, 949 (2012).

171. *See, e.g.*, Richard A. Clarke et al, *Liberty & Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence & Communications Technology* 185–86 (Dec. 12, 2013).

172. *See, e.g.*, Joby Warrick, *Iran's Natanz Nuclear Facility Recovered Quickly from Stuxnet Cyberattack*, WASH. POST, Feb. 16, 2011, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021506501.html (last accessed Aug. 3, 2016).

173. *See, e.g.*, David E. Sanger & Mark Mazzetti, *U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict*, N.Y. TIMES, Feb. 16, 2016, *available at* http://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html (last accessed Aug. 3, 2016).

174. *Heller*, 554 U.S. at 581 (*quoting* 1 DICTIONARY OF THE ENGLISH LANGUAGE, 106 (Samuel Johnson, ed.) (4th ed.) (reprinted 1978)).

175. *Id.* (quoting 1 A NEW AND COMPLETE LAW DICTIONARY (Timothy Cunningham, ed., 1771)).

176. *See* Eugene Volohk, *Implementing The Right To Keep And Bear Arms For Self-Defense: An Analytical Framework And A Research Agenda*, 56 UCLA L. REV. 1443, 1476 n. 133 (2009).

177. *See* United States v. Serrano, 2016 WL 3702744, at *4 (S.D.N.Y., June 9, 2016); Bell v. United States, 2013 WL 5763219, at *4 (E.D. Pa. Oct. 24, 2013); United States v. Smith, 2009 WL 3241992, at *1 (E.D. Mich., Oct. 8, 2009).

178. United States v. Davis, 906 F. Supp. 2d 545, 558 (S.D.W.V. 2012).

179. *Heller*, 554 U.S. at 581.

180. *See, e.g.*, N.L.R.B. v. Noel Canning, 134 S.Ct. 2550, 2578 (2014).

When we do so, the answer is clear; every viable[181] theory of the Second Amendment counsels strongly in favor of considering cryptography an arm.

B. The Purposes of the Second Amendment

Heller tells us that the prefatory clause "does not limit or expand the scope of the operative clause" but states a purpose and thus may "resolve an ambiguity in the operative clause."[182] So, the purpose of the Second Amendment can help us resolve the ambiguity in the question whether cryptography is an arm. There are a number of (sometimes overlapping)[183] theories about the Second Amendment's animating purpose, and cryptography serves each of them extraordinarily well.

1. Self-Defense

Heller recognizes self-defense as "the central component of the [Second Amendment] right itself."[184] Thus, for many, the right to self-defense, grounded in the Lockean ideal that "each man's home is his castle, and he has a natural right to defend himself, his family, and his property against threats from the outside world," animates the Second Amendment.[185] By this view, "the freedom of a state was understood at the time of the Founding to include a citizen's individual right of self defense (that is, defense of his right to life and personal security) when the state cannot assist him."[186]

Notably, the Second Amendment, by virtue of the command, "shall not be infringed," recognized a preexisting right.[187] Many think that that original right was a natural law right of self-defense, considered foundational to liberty.[188] St. George Tucker, one of the most influential early commentators on the Constitution explained: "The right of self-defense is the first right of nature: in most governments it has been the study of rulers to confine this right within the narrowest limits possible. Wherever standing armies are kept up, and the right of the people to keep and bear arms is, under any color

181. This paper deals only with theories of the Second Amendment that are broadly reconcilable with *Heller*. *Cf. Peruta*, 742 F.3d at 1155–56.

182. *Heller*, 554 U.S. at 577–78. For a thorough and clear explanation of why the prefatory clause does not limit the right, see Bradbury, et al., *supra* note 144, at 145–49.

183. *Cf.*, AMAR, *supra* note 118, at 898 ("Even with regard to the Founding, it's simplistic to deny any link between collective security and individual self-defense.").

184. *Heller*, 554 U.S. at 598.

185. Williams, *The Terrifying Second Amendment*, 101 YALE L.J. 551, 586 (1991).

186. BRADBURY, ET AL., *supra* note 131, at 159.

187. *Heller,* 554 U.S. at 592.

188. BRADBURY, ET AL., *supra* note 131, at 187.

or pretext whatsoever, prohibited, liberty, if not already annihilated, is on the brink of destruction."[189]

For those who share this view, cryptography should certainly be viewed as an arm and one protected by the Second Amendment, because it is vitally important for self-defense in the modern day. As Bruce Schneier has put it: "In a world where cyberattacks are becoming more common and more catastrophic, encryption is one of our most important defenses."[190] Even the FBI has recommended encrypting smartphones to protect oneself.[191] Currently, several U.S. Government agencies, including the Securities and Exchange Commission,[192] OnGuard Online,[193] and the Computer Emergency Response Team,[194] as well as foreign governments,[195] recommend using encryption to protect yourself. Indeed, the President's Review Group on Intelligence and Communications Technology recommended that the U.S. government promote the use of cryptography for this reason.[196]

Cryptography "is the most important privacy-preserving technology we have, and one that is uniquely suited to protect against bulk-surveillance —

189. ST. GEORGE TUCKER, 1 BLACKSTONE'S COMMENTARIES, 300 n. D (1803; reprint 1996); *see* BRADBURY, ET AL., *supra* note 131, at 159.

190. Quoted in Rob Price, *Bruce Schneier: David Cameron's Proposed Encryption Ban Would 'Destroy the Internet'*, BUSINESS INSIDER, July 6, 2015, *available at* http://www.businessinsider.com/bruce-schneier-david-cameron-proposed-encryption-ban-destroy-the-internet-2015-7#ixzz3fE7sDTh0 (last accessed July 7, 2015).

191. Trevor Timm, *The FBI Used to Recommend Encryption. Now They Want to Ban It.,* THE GUARDIAN, Mar. 28, 2015, *available at* http://www.theguardian.com/commentisfree/2015/mar/28/the-fbi-used-to-recommend-encryption-now-they-want-to-ban-it (last accessed July 13, 2015); Fed. Bureau of Investigation, *Smartphone Users Should be Aware of Malware Targeting Mobile Devices and the Safety Measures to Help Avoid Compromise,* Oct. 22, 2012, *available at* https://www.fbi.gov/sandiego/press-releases/2012/smartphone-users-should-be-aware-of-malware-targeting-mobile-devices-and-the-safety-measures-to-help-avoid-compromise (last accessed July 13, 2015).

192. *How to Protect Yourself Online,* SEC, https://www.sec.gov/spotlight/katrina/protectyourselfonline.htm (last accessed July 13, 2015).

193. *Computer Security,* OnGuard Online, http://www.onguardonline.gov/articles/0009-computer-security (last accessed July 13, 2015). OnGuardOnline.gov is managed by the Federal Trade Commission in partnership with about 15 other agencies. *See About Us*, OnGuard Online, *available at* http://www.onguardonline.gov/about-us (last accessed July 13, 2015).

194. U.S. Computer Emergency Readiness Team, *Safeguarding Your Data*, *available at* https://www.us-cert.gov/ncas/tips/ST06-008 (last accessed July 13, 2015).

195. *See e.g.*, Australian Government, *Protecting Yourself Online: What Everyone Needs to Know*, https://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/PDF%20-%20Protecting%20Yourself%20Online%20-%20Second%20Edition%20-%20Booklet.pdf (last accessed July 13, 2015).

196. CLARKE, ET AL., *supra* note 171, at 217.

the kind do ne by . . . criminals looking for vu lnerable victims."[197] "Encryption protects our data . . . . It protects our conversations, whether video, voice, or text. Itprotects our privacy. It protects our anonymity. And sometimes, it protects our lives."[198]

Because cryptography is so vital to self-defense, the Second Amendment should protect it. A particular version of the self-defense theory strengthens the case even further.

a. The Frontier

During oral argument in *Heller*, Justice Kennedy suggested that the Second Amendment had "to do with the concern of the rem ote settler to defend himself and his family against hostile Indian tribes and outlaws, wolves and bears and grizzlies and things like that."[199] In Justice Kennedy's view, "[t]he Second Amendment wasn't designed for the minutemen of the colonies to fight a tyrannical government; it was designed for the people of the frontier t o fight t he tyranny of outlaws."[200] On Justice K ennedy's frontier, "the only law that mattered was 'the law a man carried on his hip'" and, by his view, the Seco nd Amendment's role was to make sure that law wasn't stripped away.[201]

It is on the frontier, "when the sanctions of society and laws are found insufficient to restrain the violence of oppression," that the ri ght of self-defense is most applicable.[202] For, "the law, which was made for my preservation, where it cannot interpose to secure my life from present force, which if lost, is capable of no reparation, permits me my own defense."[203] So, perhaps we should not be surprised that the Founders decided to constitutionalize the right to defend oneself.[204] Professional polic e departments were still decades away,[205] and "the importance of th[e] right of

197. Bruce Schneier, *Why We Encrypt,* Foreword to Privacy Int'l et al., *Securing Safe Spaces Online: Encryption, online anonymity and human rights, available at* https://www.privacyinternational.org/sites/default/files/Securing%20Safe%20Spaces%20Online_0.pdf (last accessed July 13, 2015) at 3.

198. *Id*.

199. Transcript of Oral Argument, at 8, *Dist. of Columbia v. Heller*, 554 U.S. 570 (2008) (No. 07-290); *see also* Moore v. Madigan, 702 F.3d 933, 936 (7th Cir. 2012).

200. WINKLER, *supra* note 118, at 157.

201. *Id.* (quoting James Truslow Adams, *Our Lawless Heritage*, ATLANTIC MONTHLY, Dec. 1928, at 732).

202. 1 William Blackstone, *Commentaries* *144 (quoted in Bradbury, et al., *supra* note 131, at 145–49).

203. John Locke, *Second Treatise on Government* §§ 18–19, at 12–13 (Richard H. Cox ed., 1982) (1689) (quoted in Bradbury, et al., *supra* note 131, at 145–49).

204. LEVINSON, *supra* note 125, at 646.

205. *Id.*; *see also* DIFFIE & LANDAU, *supra* note 17, at 127–28.

self-defense was reinforced by the absence of any constitutional duty of government to defend citizens' lives, liberty, or property."[206]

Yet, when we think about the Second Amendment in that light, it appears incongruous in modern America. As Justice Scalia put it: "Undoubtedly some think that the Second Amendment is outmoded in a society where our standing army is the pride of our Nation, [and] where well-trained police forces provide personal security."[207] Justice Breyer emphasizes this point in his *Heller* dissent, arguing that the "development of modern urban police departments, by diminishing the need to keep loaded guns nearby in case of intruders, would have moved any such right [to keep handguns at home] even further away from the heart of the amendment's more basic protective ends."[208]

In modern America there are no frontiersmen, and the government has largely, if not entirely, taken over the role of protecting citizens from physical threats. But the government is woefully inadequate when it comes to protecting us from online threats. Indeed, we see time and time again that the government can hardly protect itself.[209] And often it is private entities that discover and combat major campaigns of electronic crime and espionage.[210]

As President Obama put it: "The cyberworld is the Wild Wild West — to some degree [the government is] asked to be the sheriff."[211] In other words, one must be prepared to defend oneself online: In the physical world, the need for self-defense is the exception; in cyberspace, it's the rule. As General Hayden, the former director of the CIA and the NSA, put it: "In the way we have not had to do in physical space since the closing of the frontier

206. BRADBURY, ET AL., *supra* note 131, at 145–49 (citing *DeShaney v. Winnebago Cnty. Soc. Servs. Dep't*, 489 U.S. 189, 195–97 (1989)).

207. *Heller*, 554 U.S. at 636.

208. *Id.* at 715 (J. Breyer, dissenting).

209. *See, e.g.*, Michael D. Shear & Nicole Perlroth, *U.S. v. Hackers: Still Lopsided Despite Years of Warnings and a Recent Push,* N.Y. TIMES, July 18, 2015, *available at* http://mobile.nytimes.com/2015/07/19/us/us-vs-hackers-still-lopsided-despite-years-of-warnings-and-a-recent-push.html?referrer=&_r=2 (last accessed July 20, 2015); *see also*, Nicole Perlroth, *Code Specialists Oppose U.S. and British Government Access to Encrypted Communication,* N.Y. TIMES, July 7, 2015, *available at* http://www.nytimes.com/2015/07/08/technology/code-specialists-oppose-us-and-british-government-access-to-encrypted-communication.html?smid=tw-nytimes&_r=0 (last accessed July 7, 2015) ("[G]overnment agency breaches [are] now the norm — most recently at the United States Office of Personnel Management, the State Department and the White House . . . .").

210. Ben WITTES & GABRIELLA BLUM, THE FUTURE OF VIOLENCE: ROBOTS AND GERMS, HACKERS AND DRONES: CONFRONTING NEW THREATS 68–70 (2015).

211. Nicole Perlroth & David E. Sanger, *Obama Calls for New Cooperation to Wrangle the 'Wild West' Internet,* N.Y. TIMES, Feb. 13, 2015, *available at* http://www.nytimes.com/2015/02/14/business/obama-urges-tech-companies-to-cooperate-on-internet-security.html?_r=0 (last accessed July 6, 2015).

in the nineteenth century, we're going to have to defend ourselves in cyberspace."[212]

This reality is evidenced by the ways in which private companies are preparing to defend themselves. For example, as of 2015, JPMorgan Chase had 1000 computer-security personnel, led by two retired U.S. Air Force colonels, with a quarter-billion dollar budget.[213] The bank also built a new computer-security facility near NSA headquarters in Maryland, to make it easier to lure more military talent.[214] Other financial firms have similarly inflated information-security budgets.[215] Simultaneously, venture capital investment in cybersecurity companies has skyrocketed.[216] Companies are racing (and paying) to defend themselves, because they know that they cannot rely on the government.

On this new frontier, large firms hire private armies of security experts, but ordinary civilians are left to self-defense. Here, where the government is struggling to perform its security function, we should consider cryptography an arm protected by the Second Amendment. After all, "it simply has to be the case that in a world of diminished government protection, the individual has greater latitude to take matters into his or her own hands."[217] To do so we need to be armed, which means we need cryptography.

2. The Insurrectionist Theory

Heller also embraced the "insurrectionist theory" of the Second Amendment.[218] Under this theory, grounded in both Lockean liberal and

212. General Michael Hayden, The Cybersecurity Podcast, Encryption Wars and Privacy Shield, Feb. 23, 2016, *available at* http://passcode.csmonitor.com/podcast (last accessed Mar. 4, 2014).

213. Jordan Robertson & Michael Riley, *JPMorgan Goes to War: The bank is Building a New Facility Near the NSA's Headquarters to Attract New Talent;* BLOOMBERG BUSINESSWEEK, FEB. 19, 2015, *available at* http://www.bloomberg.com/news/articles/2015-02-19/jpmorgan-hires-cyberwarriors-to-repel-data-thieves-foreign-powers (last accessed July 7, 2015).

214. *Id.*

215. Daniel Huang, Emily Glazer, & Danny Yadron, *Financial Firms Bolster Cyber Security Budgets: Survey Finds Companies Plan to Increase Spending by $2 Billion Over Next 2 Years,* WALL ST. J., Nov. 17, 2014, *available at* http://www.wsj.com/articles/financial-firms-bolster-cybersecurity-budgets-1416182536 (last accessed July 7, 2015) (noting that Citigroup, Inc. and Wells Fargo & Co. have information security budgets of approximately $300 million and $250 million respectively).

216. *See* Max Taves, *How Fear and Self-Preservation are Driving a Cyber Arms Race: Silicon Valley is Pouring More Money into Internet Security Companies than Ever Before,* CNET, May 2, 2015, *available at* http://www.cnet.com/news/how-fear-and-self-preservation-are-driving-a-cyber-arms-race/ (last accessed July 7, 2015) (reporting that venture funding for security firms in 2014 totaled $2.39 billion, representing a 35% increase over the prior year).

217. WITTES & BLUM, *supra* note 210, at 231.

218. *See Heller*, 554 U.S. at 599; *see also* Lepore, *supra* note 119.

republican ideals[219] the Second Amendment was intended to allow for an armed citizenry — "the Militia" the Amendment speaks of was "comprised all males physically capable of acting in concert for the common defense"[220] — that would act as a prophylactic against tyranny at all times, and fight against tyranny when necessary.[221] At the time the Second Amendment was penned, "[i]t was understood across the political spectrum that the right helped to secure the ideal of a citizen militia, which might be necessary to oppose an oppressive military force if the constitutional order broke down."[222] In short, according to this theory, "the republican Framers of the Second Amendment insisted on the right of all private citizens to keep arms, so as to be able to revolt."[223]

The heart of the theory is that "the ultimate "checking value" in a republican polity is the ability of an armed populace, presumptively motivated by a shared commitment to the common good, to resist government tyranny."[224] Common armament, James Madison argued, was an advantage Americans had over all other people.[225] Justice Story viewed it "as the palladium of the liberties of a republic; since it offers a strong moral check against the usurpation and arbitrary power of rulers; and will generally, even if these are successful in the first instance, enable the people to resist and triumph over them."[226]

This insurrectionist view makes intuitive sense, given that the Second Amendment's Framers "had some first hand experience with the benefits of the militia in resisting tyranny."[227] In James Madison's opinion "[t]hose who are best acquainted with the late successful resistance of this country against the British arms" would realize that no federal government turned tyrannical could hope to succeed in oppressing the Militia.[228] So, the theory goes, "if Congress should ever use standing armies to advance tyrannical designs, they would be outnumbered and outfought by liberty-loving militia

219. *See* Williams, *supra* note 202, at 584.

220. *Heller*, 554 U.S. at 595 (quoting *United States v. Miller*, 307 U.S. 174, 179 (1939)).

221. *See* LEVINSON, *supra* note 125, at 657.

222. *Heller*, 554 U.S. at 599.

223. WILLIAMS, *supra* note 202, at 584 (describing Levinson, *supra* note 125).

224. LEVINSON, *supra* note 125, at 648; *see also* Brent J. McIntosh, *The Revolutionary Second Amendment*, 51 ALA. L. REV. 673, 674 (2000).

225. THE FEDERALIST NO. 46 at 299 (J. Madison) (Clinton Rossiter ed., 1961).

226. 3 J. STORY, COMMENTARIES § 1890 (1883) (quoted in Levinson, *supra* note 125, at 649).

227. WILLIAMS, *supra* note 185, at 581.

228. THE FEDERALIST NO. 46 at 299 (J. Madison) (Clinton Rossiter ed. 1961); *see* Bradbury, et al., *supra* note 131, at 179.

members."[229] For that vision to co me to pass, especiall y today, the Militia would need cryptography.

a. Cryptography and Revolutions

In the coloni es, there would have been little use for cry ptography in day-to-day life. "Revolutions, howeve r, provide fertile soil for intrigue, espionage, and, of course , secret communications."[230] And am ong those who appreciated the im portance of cr yptography in revolution were the Second Amendment's Framers.[231] Thr oughout the Revolutionary period, American political figures used various forms of cryptography to protect both public and private correspondence.[232]

"America was born of a revolutionary conspiracy" and "the young nation's leaders . . . turned to codes and ciphers in an effort to preserve the confidentiality of their communications."[233] Cryptography was a vital weapon of resistance for the American colonists and the Founding Fathers "viewed secret writing as an essential instrument for protecting critical information in wartime."[234] Even before the Revolution broke out, colonists used cryptography to evade the English censors.[235] G overnment agents commonly opened and read mail, driving men like Thomas Jefferson to encipher their correspondence.[236] Benjamin Franklin even printed a textbook on the encryption techniques of the day.[237] In N ovember of 177 5, the Continental Congress established the Committee of Secret C orrespondence — which included key figures like

229. WILLIAMS, *supra* note 185, at 576.

230. RALPH E. WEBER, MASKED DISPATCHES: CRYPTOGRAMS AND CRYPTOLOGY IN AM. HISTORY, 1775–1900 xii (1993); *see also* Ralph E. Weber, *A Masked Dispatch*, 14 CRYPTOLOGIA, 374–80 (1990); Ralph E. Weber, *James Lovell and Secret Ciphers During the American Revolution,* 2 CRYPTOLOGIA 75–88 (1978).

231. *See* John A. Fraser, III, *The Use of Encrypted, Coded and Secret Communications is an "Ancient Liberty" Protected by the United States Constitution,* 2 V A. J.L. & TECH. 2, 21 (1997); WEBER, MASKED DISPATCHES, *supra* note 252, at xii; Jennifer Wil cox, *Revolutionary Secrets: Cryptology in the American Revolution,* https://www.nsa.gov/about/cryptologic-heritage/historic al-figures-publications/publications/pre-wwii/assets/files/Revolutionary_Secrets_2012.pdf (last visited Oct. 14, 2015).

232. FRASER, *supra* note 231, at 21–40.

233. *Id.* at 21 (quoting David W. Gaddy, *Introduction*¸ in WEBER, MASKED DISPATCHES, *supra* note 230).

234. WEBER, MASKED DISPATCHES, *supra* note 230.

235. FRASER, *supra* note 231, at 20.

236. *Id.*

237. *Id.*

Franklin, and John Jay — and tasked it with engaging with rebel sympathizers oversees, intelligence missions, and the development of codes and ciphers.[238]

As it was to the American Revolution, secrecy is key to most rebellions. Surprise attack and misdirection are the bread and butter of insurgent forces. "Guerrillas are masters of the arts of simulation and dissimulation; they create pretenses and simultaneously disguise or conceal their true semblance."[239] And the ability to keep information from the enemy is among the guerrillas' most important traits.[240] As Chairman Mao wrote, "[t]he movements of guerilla troops must be secret and of supernatural rapidity; the enemy must be taken unaware, and the action entered speedily."[241] Che Guevara similarly emphasized surprise and secrecy.[242] Guevara taught that the guerrilla soldier:

> ought to be close-mouthed. Everything that is said and done before him should be kept strictly in his own mind. He ought never to permit himself a single useless word, even with his own comrades in arms, since the enemy will always try to introduce spies into the ranks of the guerrilla band in order to discover its plans, locations, and means of life.[243]

Guevara tells us that in preparing for an insurgency "[a]bsolute secrecy, a total absence of information in the enemy's hands, should be the primary base of the movement."[244] It is only secrecy that allows insurgents to compete with the professional militaries of nation-states.[245]

And because secrecy is key, cryptography is key. Paul Revere used code to signal the British mode of advance. Lawrence of Arabia used British codes during the Arab Revolt.[246] Russian nihilists developed their own

238. Central Intelligence Agency, *A Look Back . . . Intelligence and the Committee of Secret Correspondence,* https://www.cia.gov/news-information/featured-story-archive/2011-featured-story-archive/intelligence-and-the-committee-of-secret-correspondence.html (last visited Oct. 12, 2015); *see also* Fraser, *supra* note 231, at 20.

239. Samuel B. Griffith, MAO TSE-TUNG, ON GUERRILLA WARFARE, 26 (trans. with Introduction by Samuel B. Griffith), (2007).

240. *See id.* at 23.

241. *See id.* at 97.

242. ERNESTO CHE GUEVARA, GUERRILLA WARFARE 13–15, 26, 35–37, 52–53, 57, 60, 63, 69, 109–13 (2012).

243. *Id.* at 37.

244. *Id.* at 110.

245. *See* Dr. Lt. Col. David Kilcullen, *Twenty-Eight Articles: Fundamentals of Company-Level Counterinsurgency*, *available at* http://www.au.af.mil/info-ops/iosphere/iosphere_summer06_kilcullen.pdf (last visited Nov. 6, 2015).

246. DAVID KAHN, THE CODEBREAKERS 312 (1996).

encryption schemes,[247] as did European anti-monarchical societies.[248] All sides in the Mexican Revolution employed cryptography.[249] The Irish Republican Army encrypted messages between its members.[250]

Of course, in rebellion, secrecy is a matter of life or death, and so cryptography is too. Mary, Queen of Scots was beheaded after her encrypted communications about a plot to assassinate Queen Elizabeth and install Mary on the throne were deciphered.[251] French Huguenot insurgents relied on cryptography through the wars of religion, before eventually being forced to surrender Realmont after the Royal Army decrypted their messages.[252] And many of those active in the Resistance during the Second World War lost their lives as a result of failing to use adequate cryptography.[253]

Moreover, if cryptography was important to rebels in the past, it is even more so now. Given the immense power of modern surveillance, cryptography is one of the only ways to hope to ensure secrecy in the modern era.[254] This is why the U.S. government has taught Iranian Mujahedeen-e-Khalq fighters to use cryptography, along with small-unit tactics and weapons training.[255] Similarly, the government has urged the use of Tor by the Syrian rebels battling Bashar al-Assad,[256] and has trained them to encrypt their internet chats and their computers.[257] And Edward Snowden uses cryptography in his attempts to evade the American national security apparatus.[258]

247. *Id.* at 620–21.

248. *Id.* at 772–73.

249. José De Jesús Angel Angel & Guillermo Morales-Luna, *Cryptographic Methods During the Mexican Revolution,* 33 CRYPTOLOGIA 188–96 (2009).

250. Stephen Budiansky, *Review of Decoding the IRA by Tom Mahon and James J. Gillogly*, 33 CRYPTOLOGIA 292–94 (2009).

251. VAGLE, *supra* note 2, at 108 (citing SINGH, *supra* note 9, at 32–44).

252. *Id.* at 107 n.33 (citing KAHN, *supra* note 246, at 157).

253. *See* HASTINGS, *supra* note 165, at 264, 267–69, 273.

254. *See* Peter Swire & Kenesa Ahmad, *Encryption & Globalization,* 13 COLUM. SCI. & TECH. L. REV. 416, 470–473 (2012).

255. Seymour M. Hersh, *Our Men in Iran?,* THE NEW YORKER (Apr. 5, 2012), *available at* http://www.newyorker.com/news/news-desk/our-men-in-iran (last visited July 28, 2015).

256. HARRIS, *supra* note 86, at 86.

257. Jay Newton-Small, *Hillary's Little Startup: How the U.S. is Using Technology to Aid Syria's Rebels* (June 13 , 2012), *available at* http://world.time.com/2012/06/13/hillarys-little-startup-how-the-u-s-is-using-technology-to-aid-syrias-rebels/ (last visited July 28, 2015).

258. *See, e.g.*, James Banford, *The Most Wanted Man in the World*, WIRED, *available at* https://www.wired.com/2014/08/edward-snowden/#ch-7 (last visited Aug. 3, 2016); Micah Lee, *available at* https://theintercept.com/2014/10/28/smuggling-snowden-secrets/ (last visited Aug. 3, 2016).

b. The Paradoxical Prefatory Clause

Heller embraced both the insurrectionist and self-defense theories of the Second Amendment. The two are linked by the idea that when citizens rise up, the weapons they have to fight with will be the ones they keep for self-defense.[259] In many ways however those two purposes have diverged as military technology has developed. It is hard to imagine a citizen-militia, armed with weapons commonly used for self-defense, defeating the U.S. military.[260] As *Heller* states:

> It may well be true today that a militia, to be as effective as militias in the 18th century, would require sophisticated arms that are highly unusual in society at large. Indeed, it may be true that no amount of small arms could be useful against modern-day bombers and tanks. But the fact that modern developments have limited the degree of fit between the prefatory clause and the protected right cannot change our interpretation of the right.[261]

This is the "symmetry problem" that Brent McIntosh has explained.[262] "Effectuating the purpose of the Second Amendment presupposes some rough proportionality between the arms available to Americans and the weapons held by those against whom Americans are to defend themselves."[263] And the problem arises because the arms used for war and self-defense have diverged since 1789.[264]

Cryptography, however, is an exception to this trend. It is equally well suited to self-defense against criminals and battling oppressive regimes. The cryptography many citizens use every day for self-defense is effectively as sophisticated as the cryptography used by major governments and

259. *See Heller*, 554 U.S. at 625.

260. *See, e.g.*, Robert J. Cottrol & Raymond T. Diamond, *The Second Amendment: Toward an Afro-Americanist Reconsideration,* 80 GEO. L.J. 309, 315–17 (1991); *see also The West Wing: Six Meetings Before Lunch,* (NBC television broadcast Apr. 5, 2000) (President Bartlet: "Do you think I could take George Washington?" Charlie: "Take him at what, sir?" President Bartlet: "I don't know. . . a war?" Charlie: "Could you have taken George Washington in a war?" Bartlet: "Yeah." Charlie: "Well, you'd have the Air Force and he'd have the Minutemen, right?" President Bartlet: "The Minutemen were good." Charlie: "Still, I think you could probably take him.");

261. *Heller*, 554 U.S. at 627–28.

262. MCINTOSH, *supra* note 224, at 692–93.

263. *Id.*

264. *Id.* at 697; *Heller*, 554 U.S. at 627–28.

militaries,[265] and is useful against them.[266] Indeed, if the cryptography that individuals are using was not effective against government agencies, we would not be having this discussion at all.

3. "God created men. Colonel Colt made them equal."[267]

In an influential 1991 article, Robert J. Cottrol and Raymond T. Diamond have argued that the Second Amendment should be analyzed "with an eye toward subcultures in American society who have been less able to rely on state protection."[268] Justice Thomas emphasized this theory in his *McDonald* concurrence.[269] And history supports them.

In England, prior to the Revolution, the right to arms was "highly circumscribed by the English class structure."[270] Indeed, the Game Act deprived most English subjects the right.[271] This led Blackstone to complain that "fifty times the property [was] required to enable a man to kill a partridge, as to vote for a knight of the shire."[272] This was, of course, a method of social control of the masses, who "[t]he law often regarded . . . as a dangerous class, useful perhaps in defending shire and realm, but also capable of mischief with their weapons, mischief towards each other, toward their betters, and toward their betters' game."[273]

Discriminatory limits on the English right to bear arms were also based on religious distinctions: Catholics were seen as potentially subversive and thus often denied the right.[274] And it was the attempt of King James II — England's last Catholic monarch — to disarm Protestants that led to the incorporation into the English Bill of Rights of its seventh provision: "That the Subjects which are [P]rotestants may have [A]rms for their [D]efence suitable to their [C]onditions, and as allowed by [L]aw."[275]

265. *See, e.g.,* Christopher Soghoian, *Lawfare Podcast Episode #98 Chris Soghoian Responds to FBI Director Comey* (Oct. 30, 2014), *available at* http://www.lawfareblog.com/2014/11/the-lawfare-podcast-episode-98-chris-soghoian-responds-to-fbi-director-james-comey/ (last visited May 29, 2015); Clarke, et al., *supra* note 171, at 186–87.

266. *See, e.g.,* SCHNEIER, *supra* note 197, at xix.

267. WINKLER, *supra* note 118, at 161. (This was a Colt marketing slogan and a common saying on the frontier. It also reflects the views of the 14th Amendment's framers). *See id.* at 142.

268. COTTROL & DIAMOND, *supra* note 260, at 319.

269. *See McDonald*, 561 U.S. at 844 (Thomas, J., concurring).

270. COTTROL & DIAMOND, *supra* note 260, at 321.

271. Bradbury, et al., *supra* note 131, at 169.

272. 4 WILLIAM BLACKSTONE, COMMENTARIES *175.

273. COTTROL & DIAMOND, *supra* note 260, at 321; Bradbury, et al., *supra* note 131, at 205.

274. *Id.*

275. BRADBURY, ET AL., *supra* note 131, at 168.

The English right thus codified class and religious distinctions anathema to American ideals. For this reason, early American commentators praised the Second Amendment as more egalitarian than, and thus superior to, its English counterpart.[276] St. George Tucker exalted the Second Amendment for being a right of the whole of the people "without any qualification as to their condition or degree, as is the case in the British government."[277] The British version, he argued, kept "the mass of the people" "in a state of the most abject subjugation," while "in America we may reasonably hope that the people will never cease to regard the right of keeping and bearing arms as the surest pledge of their liberty."[278]

In theory, the Second Amendment, unlike the British right, was a democratic one. "Those who had been part of the suspect classes in England — the poor, religious dissenters, and others who had traditionally only enjoyed a qualified right to possess arms — found the right to be considerably more robust in America."[279] However, they had been replaced with a new racial underclass, whose "right to possess arms was highly dependent on white opinion of black loyalty and reliability."[280] Restrictions on the extension of the right to keep and bear arms to Blacks varied by time and place, but were always animated by the omnipresent specter of slave rebellion.[281]

"After the Civil War, Southern anxiety about an uprising among the newly freed slaves peaked. As Representative Thaddeus Stevens is reported to have said, '[w]hen it was first proposed to free the slaves, and arm the blacks, did not half the nation tremble?'"[282] This set off "systematic efforts in the old Confederacy to disarm the more than 180,000 freedmen who had served in the Union Army, as well as other free blacks."[283] Southern States passed Black Codes, which dramatically limited the rights of freedmen to

276. *Id.* (citing WILLIAM RAWLE, A VIEW OF THE CONSTITUTION OF THE UNITED STATES OF AMERICA 125–26 (2d ed. 1829; reprint 1970).

277. 2 Tucker's Blackstone at *143–44 & nn. 40–41; Bradbury, et al., *supra* note 131, at 205.

278. 2 Tucker's Blackstone at *414 n 3; Bradbury, et al., *supra* note 131, at 205.

279. Cottrol & Diamond, *supra* note 260, at 326.

280. *Id.*

281. *See id.* at 331–39; *McDonald*, 561 U.S. at 844 (Thomas, J., concurring) ("It is difficult to overstate the extent to which fear of a slave uprising gripped slaveholders and dictated the acts of Southern legislatures."); *id.* at 845 (Thomas, J., concurring) ("The fear generated by these and other rebellions led Southern legislatures to take particularly vicious aim at the rights of free blacks and slaves to speak or to keep and bear arms for their defense.").

282. *McDonald*, 561 U.S. at 844 (Thomas, J., concurring) (quoting K. STAMPP, THE ERA OF RECONSTRUCTION, 1865–1877, 104 (1965)).

283. *Id.* at 847 (Thomas, J., concurring) (quoting *id.* at 771) (internal quotation marks omitted); WINKLER, *supra* note 118, at 139.

keep and bear arms.[284] "Additionally, throughout the South, armed parties, often consisting of ex-Confederate soldiers serving in the state militias, forcibly took firearms from newly freed slaves."[285]

This mass disarmament was of great concern to those fighting for the civil rights of the newly freed slaves.[286] "For them, the right of the black population to possess weapons was not merely of symbolic and theoretical importance; it was vital . . . [as] a means of preventing virtual reenslavement of those formerly held in bondage."[287] Indeed, it was a major impetus in the northern Republican push for applying the Bill of Rights to the states.[288] Fredrick Douglas himself believed that abolition would not be complete until the Constitution protected the right of blacks to keep and bear arms.[289]

The situation was clear: "When guns were outlawed, only Klansmen would have guns."[290] And "[t]he use of firearms for self-defense was often the only way black citizens could protect themselves from mob violence."[291] Thus, for some, the animating principle of the Second Amendment lies in protecting Blacks from racial violence and oppression in the Deep South. For them "the poster boy of arms" is not "the Concord minuteman [but] the Carolina freedman."[292] This theory is a sort of hybrid of the self-defense and insurrectionist theories, by which the Second Amendment assures individuals the means to defend themselves from violence, whether public, private, or both. Such a reading was particularly necessary at the time, because the line between public and private violence was blurry in the reconstruction South, where "sometimes the sheriff wore a badge; sometimes he wore a sheet."[293]

The (putatively) democratic nature of the American right implies both that it enabled the people to protect themselves against the usurpation of

284. *See McDonald*, 561 U.S. at 847 (Thomas, J., concurring); Cottrol & Diamond, *supra* note 260, at 344–45; Bradbury, et al., *supra* note 131, at 223–24.

285. *McDonald*, 561 U.S. at 844 (Thomas, J., concurring) (quoting *id.* at 772) (internal quotation marks and brackets omitted).

286. WINKLER, *supra* note 118, at 139.

287. COTTROL & DIAMOND, *supra* note 260, at 345.

288. *Id.* at 345–46; Bradbury, et al., Bradbury, et al., *supra* note 131, at 224–25.

289. *In What New Skin Will the Old Snake Come Forth? An Address Delivered in New York, New York, May 10, 1865*, reprinted in 4 THE FREDERICK DOUGLASS PAPERS 79, 83–84 (J. Blassingame & J. McKivigan eds., 1991).

290. AMAR, *supra* note 118, at 899.

291. *McDonald*, 561 U.S. at 857 (Thomas, J., concurring).

292. AHKIL AMAR, THE BILL OF RIGHTS, 266 (1994).

293. Darrel A.H. Miller, *Retail Rebellion and the Second Amendment,* 86 IND. L.J. 939, 945–46 (2011); *see also McDonald*, 561 U.S. at 779 (Alito, J., majority), 847 (Thomas, J., concurring), 855–56 (Thomas, J., concurring); Amar, *supra* note 118, at 899; Cottrol & Diamond, *supra* note 260, at 319, 348.

power by the few; and that it enabled the few to protect themselves against the violence of the many.[294] The American Revolution dramatized the former role. The civil rights struggle, from the antebellum period through the Sixties, dramatized the latter. In the 1960s the Black Panthers seized on the Second Amendment as a tool in the struggle, bringing arms into California's capitol and "patrolling" the police.[295]

Particularly for those whose view of the Second Amendment is motivated by the image of the Carolina freedman, cryptography should be considered an arm. Perhaps cryptography would have been of little more use to the Carolina freedman than the Montana pioneer. But it might be an especially useful tool of self-defense minorities of thought: political dissidents; religious minorities; and those who love people they're not supposed to.[296] As the U.N.'s special rapporteur on freedom of opinion and expression put it, cryptography can

> provide individuals with a means to protect their privacy, empowering them to browse, read, develop and share opinions and information without interference and enabling journalists, civil society organizations, members of ethnic or religious groups, those persecuted because of their sexual orientation or gender identity, activists, scholars, artists and others to exercise the rights to freedom of opinion and expression.[297]

It can protect those reading heretical religious texts, studying subversive political tracts, or viewing niche pornography, regardless of whether they face persecution from a state or private members of an intolerant society.[298] It can protect those same groups as they seek to discuss their unwelcome ideas with others, whether converting them, organizing them, or seducing them.[299] And for these people, privacy is also a matter of physical security.

294. In his *Abridgement* of his three volume *Commentaries*, Justice Story listed the Second Amendment among those "properly" included in the Bill of Rights (he would have excluded the Fifth, Sixth, and Seventh, which relate to judicial procedure). These "proper" rights served three purposes, one of which was the protection of minorities. Bradbury, et al., *supra* note 131, at 208 (citing JOSEPH STORY, COMMENTARIES ON THE CONSTITUTION OF THE UNITED STATES §§ 980–982, at 695 (Ronald D. Rotunda & John E. Nowak, eds., 1833, reprint 1987)).

295. WINKLER, *supra* note 118, at 230–44.

296. As will be discussed later, the Second Amendment right here begins to blend with the First Amendment rights to expression and association.

297. U.N. HUMAN RIGHTS COUNCIL, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*, A/HRC/29/32, (May 22, 2015.), http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx

298. *Id.* at 5–6.

299. *See id.* at 7–8.

It is because cryptography is so useful against repressive governments that the State Department funds Tor, the anonymous web-browsing client, and other "counter-censorship and secure communications technology."[300] Between 2008 and 2013, the State Department spent over $100 million on programs that involved the distribution of cryptographic software, designed to allow activists and dissidents to "exercise their human rights freely and safely online."[301] Moreover "[d]uring the Arab Spring [the State Department] train[ed] people to use tools like Tor to escape censorship and retaliation."[302] The program under which Washington trained Syrian rebels in encryption grew out of an aborted plan to teach similar techniques to religious dissidents in China.[303]

As it is, dissidents, journalists, and others who must worry about what they say commonly use Tor to evade China's ubiquitous internet surveillance.[304] Those working for Tibetan independence rely on cryptography to keep their messages secret, and themselves safe.[305] Iranian activists did the same during the 2009 protests.[306] Groups like Freedom House recommend that human rights activists use encryption in repressive countries.[307] Many other, less prominent, dissident groups around the world use PGP, Skype, and other widely available cryptographic methods to evade government surveillance.[308] Others are developing communications systems relying on cryptography precisely for communicating in the face of

300. Andrea Peterson, *The NSA is Trying to Crack Tor. The State Department is Helping Pay For It.*, WASH. POST (Oct. 5, 2013), https://www.washingtonpost.com/blogs/the-switch/wp/2013/10/05/the-nsa-is-trying-to-crack-tor-the-state-department-is-helping-pay-for-it/; Dune Lawrence, *The Inside Story of Tor, the Best Internet Anonymity Tool the Government Ever Built,* BLOOMBERG BUSINESS (Jan. 23, 2014), http://www.bloomberg.com/bw/articles/2014-01-23/tor-anonymity-software-vs-dot-the-national-security-agency#p1.

301. Clarke, et al., *supra* note 171, at 217.

302. *Id.*; *see also* Newton-Small, *supra* note 257.

303. NEWTON-SMALL, *supra* note 257.

304. Dimitri Vitaliev, *Vaulting the great firewall,* THE GUARDIAN (Aug.5, 2008), http://www.theguardian.com/commentisfree/2008/aug/05/china.censorship; Lawrence, *supra* note 300.

305. Vagle, *Furtive Encryption*, *supra* note 2, at 107 n. 34 (citing KAHN, *supra* note 268, at 84); *Tibet- the cyber wars* (Mar. 24, 2008), http://www.bbc.co.uk/blogs/technology/2008/03/tibet_the_cyber_wars.html.

306. LAWRENCE, *supra* note 300.

307. Cynthia Romero, *What Next? The Quest to Protect Journalists and Human Rights Defenders in a Digital World*, FREEDOM HOUSE, 8 (2014), https://freedomhouse.org/sites/default/files/What%27s%20Next%20%20The%20Quest%20to%20Protect%20Journalists%20and%20Human%20Rights%20Defenders%20in%20a%20Digital%20World.pdf; Stephanie Hankey & Daniel O Clunaigh, *Rethinking Risk and Security of Human Rights Defenders in a Digital Age,* 5 J. HUM. RTS. PRAC. 535, 539 (2013).

308. *See* Oliver Leistert, *Resistance against Cyber-Surveillance within Social Movements and how Surveillance Adapts,* 9 SURVEILLANCE & SOCIETY, 441, 446–47 (2012).

tyranny.[309] And, coming full circle, there has been a recent effort in the United States to increase familiarity with cryptography in the Black community.[310]

In keeping with this theme, encryption can be particularly useful for women to protect themselves from gender-based violence. It is an important tool for domestic violence survivors seeking to escape from their tormentors.[311] And it can be used to help women defend themselves from online sexual violation. Women are most frequently the victims of non-consensual pornography — the dissemination of sexually explicit images without consent.[312] And nonconsensual pornography has especially severe consequences for women.[313] It can severely damage victims' career prospects; lead to anxiety; depression and anorexia; and harassment, both online and offline.[314] It can also be used to extort victims, either for money or for additional explicit materials.[315] Cryptography may not protect women when the perpetrator of nonconsensual pornography is an ex, or someone else who obtained the images with the victim's consent.[316] However, in some circumstances — including the publication of celebrities' nude photos that kicked off round two of the cryptowars — the photos may be published by a hacker who stole intimate photos stored on the victim's phone or computer.[317] In those situations, women can use cryptography to defend themselves.[318]

309. *See* Soulaf Saab, et al, *Secure Cryptographic Mechanisms for Safeguarding Citizen Communications in the Presence of Tyranny,* 2 INT'L J. INFO. SEC. RESEARCH (2012).

310. Adrianne Defries, *The Black Community Needs Encryption,* MOTHERBOARD (DEC. 11, 2015), https://motherboard.vice.com/read/the-black-community-needs-encryption?utm_source=mbtwitter.

311. *See* LAWRENCE, *supra* note 300.

312. *See* Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 346, 353 (2014).

313. *See id.*

314. *Id.* at 350–52.

315. Benjamin Wittes, et al., *Sextortion: Cybersecurity, teenagers, and remote sexual assault* (May, 2016), http://www.brookings.edu/~/media/Research/Files/Reports/2016/05/sextortion/sextortion1.pdf?la=en.

316. *See* CITRON & FRANKS, *supra* note 312, at 346.

317. *See e.g.*, Wittes, et al., *supra* note 315, at 2, 10, 19–20; Andrea Peterson, Emily Yahr and Joby Warrick, *Leaks of nude celebrity photos raise concerns about security of the cloud* (Sept. 1, 2014), https://www.washingtonpost.com/politics/leaks-of-nude-celebrity-photos-raise-concerns-about-security-of-the-cloud/2014/09/01/59dcd37e-3219-11e4-8f02-03c644b2d7d0_story.html; Benjamin Wittes & Mona Sedky, *The Lawfare Podcast: Mona Sedky on Prosecuting Sextortion* (June 25, 2016), https://www.lawfareblog.com/lawfare-podcast-mona-sedky-prosecuting-sextortion ("Many of the sextortion cases involve hacking.").

318. *See* Keith Stuart, *How to Protect Your Digital Photos from Hackers,* THE GUARDIAN (Sept. 3, 2014), https://www.theguardian.com/technology/2014/sep/03/how-to-protect-your-digital-photos-from-hackers.

a. Collective Defense in "the Era of DIY Signals Counterintelligence"[319]

In part, the Second Amendment envisioned that the people would contribute to the collective defense of the United States against foreign aggressors.[320] In light of Cold War era mutually assured destruction, and post-Cold War American hegemony, that the Militia might be necessary to combat foreign aggressors seems absurd. And it may be, with regard to kinetic battles. However, a citizenry armed with cryptography is important for defending the homeland against foreign aggression, not in some dystopian future, but today.

The face of national security has changed drastically since the dawn of the internet era. More and more combat takes place online and the distinction between military and civilian targets is constantly eroding. For examples of this, one need only look to the state-sponsored data breaches at the Office of Personnel Management, American Airlines, Anthem Inc., and Sony Corp. Perhaps the best example is large-scale intellectual theft from American industry.[321] "Foreign intelligence agencies have been penetrating American corporate networks and stealing technology electronically since the 1990s."[322] General Keith Alexander has called Chinese industrial espionage "the greatest transfer of wealth in history."[323] These thefts from private companies obviously implicate national security in a national interest and economic sense.[324]

However, these thefts also implicate national security in ways that matter to the warfighter on the ground, because many of our classified military secrets sit on the private networks of American industry.[325] A war with China could see American pilots flying F-35s against remarkably similar planes and pilots that know the F-35's weaknesses.[326] That is because Chinese hackers stole huge amounts of technical and design information about the F-35 — the most advanced, most expensive, fighter ever built — from the networks of Lockheed Martin and its subcontractors.[327] The F-35 is hardly the only example of this. "Every branch of the US Armed Forces

319. WITTES & BLUM, *supra* note 210, at 69.

320. *See* MCINTOSH, *supra* note 224, at 683.

321. Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare,* 45–53 (2011); DIFFIE & LANDAU, *supra* note 17, at 5.

322. BRENNER, *supra* note 321, at 45.

323. HARRIS, *supra* note 86, at 53.

324. *See id.* at 53.

325. BRENNER, *supra* note 321, at 63.

326. *See* HARRIS, *supra* note 86, at xiv–xv.

327. *See id.* at x–xv.

ha[s] been compromised, along with the technology and weapons that the United States use[s] to fight in every domain — land, air, sea, and space."[328]

Furthermore, the bulk of American critical infrastructure is in private hands and vulnerable to electronic attack.[329] Policy makers tremble at the thought that an electronic attacker "could hijack the Internet-connected devices that regulate the flow of electrical power and plunge our cities into darkness."[330] Foreign hackers have already probed the infrastructure controlling our electrical grid, and in other countries electronic attacks have caused power-outages.[331] The same could happen here.[332] Indeed, it may have already happened; at least some officials believe foreign hackers were responsible for major blackouts in 2003 and 2008 (although they likely triggered the power outages accidently while exploring the system).[333] The financial system — also supported by private networks — is similarly vulnerable; an adversary could cause "a national panic" by "erasing or corrupting the data in financial accounts."[334] Perhaps most frightening, nuclear facilities could be attacked as well.[335]

Most American computer networks are private, and the government cannot hope to secure them by itself.[336] In light of this merging of public and private security, we need "an engaged and mobilized citizenry — a true bottom-up awareness and willingness to act in the interests of security."[337] "Counterintelligence used to be the stuff of government spies and nation-states; it was the concern of the CIA, the FBI, and the military. It is now a concern for every organization that lives on electronic networks and has secrets to keep."[338] Ordinary people will have to be involved in security, which often means simply keeping themselves secure. That includes using

328. *See id.* at 140.

329. *See* WITTES & BLUM, *supra* note 210, at 227; Michael Assante, *America's Critical Infrastructure Is Vulnerable To Cyber Attacks*, FORBES (Nov. 11, 2014), http://www.forbes.com/sites/realspin/2014/11/11/americas-critical-infrastructure-is-vulnerable-to-cyber-attacks/.

330. HARRIS, *supra* note 86, at xii.

331. *Id*. at 155.

332. *See* Kim Zetter, *Everything We Know About Ukraine's Power Plant Hack*, WIRED (Jan. 20, 2016), http://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/.

333. HARRIS, *supra* note 86, at 52–53.

334. *Id*. at xx.

335. NUCLEAR THREAT INITIATIVE, NTI NUCLEAR SECURITY INDEX: BUILDING A FRAMEWORK FOR ASSURANCE, ACCOUNTABILITY, AND ACTION 4 (3rd ed. Jan. 2016).

336. HARRIS, *supra* note 86, at xx.

337. WITTES & BLUM, *supra* note 210, at 226.

338. BRENNER, *supra* note 321, at 64.

strong passwords and updating software.[339] It also includes using strong cryptography.

Writing from a national security standpoint, Joel Brenner recommends that companies encrypt all of their sensitive data in order to protect themselves and the country in a networked world.[340] Richard Clarke recommends encrypting the signals in and out of the power-grid's control systems to protect critical infrastructure.[341] On a more micro level, using cryptography to safeguard the privacy of individuals can have national security implications. For example, both civilian and government networks are often penetrated through "spearphishing": an unsuspecting employee clicks on a link in an email that appears to come from a trusted source.[342] The more attackers know about the target and the purported sender, the more carefully they can craft their attacks and the more likely they are to succeed. Private use of cryptography can protect those personal details from being used by the would-be attackers.

Indeed, a contributing factor to the end of the original crypto-wars may have been that "the national-security establishment decided that the widespread use of strong encryption . . . was, in the end, ultimately in the nation's interest."[343] That is the same conclusion that the President's Review Group on Intelligence and Communications Technologies came to in 2013.[344] That group issued "recommendations . . . designed to protect our national security and advance our foreign policy while also respecting our longstanding commitment to privacy and civil liberties . . ."[345] Among its conclusions was that, "[t]he use of reliable encryption software to safeguard data is critical to many sectors and organizations, including financial services, medicine and health care, research and development, and other critical infrastructures in the United States . . ." and therefore

> the US Government should: (1) fully support and not undermine efforts to create encryption standards; (2) not in any way subvert, undermine, weaken, or make vulnerable generally available commercial software; and (3) increase the use of encryption and

339. WITTES & BLUM, *supra* note 210, at 227.

340. BRENNER, *supra* note 321, at 241–42.

341. RICHARD A. CLARKE, CYBERWAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 169 (2010). *See also*, *id.* at 174. (recommending all information on all Department of Defense computers should be encrypted).

342. *See e.g.*, HARRIS, *supra* note 86, at xvi, 129, 155, 187.

343. DIFFIE & LANDAU, *supra* note 17, at 9; *see also* DAM & LIN, *supra* note 4, at xiii;

344. Clarke et al, *supra* note 171, at 216–19.

345. *Id*. at 1–2.

> urge US companies to do so, in order to better protect data in transit, at rest, in the cloud, and in other storage.[346]

Similarly, General Michael Hayden, the former Director of both the CIA and the NSA, Admiral Mike McConnell, the former director of the NSA and DNI, and Michael Chertoff, the former secretary of Homeland Security have all said that widespread, strong encryption is important for the national security of the United States.[347]

b. A Structural Point

In a 2004 opinion, the Office of Legal Counsel ("OLC") laid out the argument for the "individual right" view under the Second Amendment that was eventually adopted in *Heller*.[348] That opinion includes a structural argument for the "individual right" view that also weighs in favor of considering cryptography an "arm" protected by the Second Amendment. OLC argued that the Second Amendment exists in "a subset of the Bill of Rights amendments, the First through Fourth, that relates most directly to personal freedoms,"[349] which allow Americans "to act without undue governmental interference."[350] As the opinion points out, the Second Amendment is "useful for protecting not only the citizen's person but also the 'houses' that the Third and Fourth Amendments guard."[351]

Similarly, if cryptography is considered an "arm," the Second Amendment would be useful for protecting the privacy interest in what happens in our "houses" — which the Third and Fourth also protect — as well as the rights to anonymous speech and association — which the First Amendment protects.[352] As Phil Zimmerman wrote: "[I]n the Information Age, cryptography is about political power, and, in particular, about the power relationship between a government and its people. It is about the right to privacy, freedom of

346. *Id.* at 216.

347. *Episode 11: Encryption Wars and Privacy Shield*, THE CYBERSECURITY PODCAST (Feb. 23, 2016), http://passcode.csmonitor.com/podcast.

348. Bradbury et al., *supra* note 131, at 127.

349. *Id.* at 161.

350. *Id.* at 162; *see also Griswold v. Connecticut*, 381 U.S. 479 (1965) (drawing on the First, Third, Fourth and Fifth Amendments, and their "penumbra and emanations" in finding a constitutionally protected right to privacy).

351. BRADBURY ET AL., *supra* note 131, at 162.

352. *See e.g.*, LESSIG, *supra* note 75, at 67; Gwynne B. Barrett, *The Law of Diminishing Privacy Rights: Encryption Escrow and the Dilution of Associational Freedoms in Cyberspace,* N.Y.L. SCH. J. HUM. RTS. 115 (1998); Jill M. Ryan, *Freedom to Speak Unintelligibly: The First Amendment Implications of Government-Controlled Encryption,* 4 WM. & MARY BILL RTS. J. 1165 (1996); *see also* U.N. HUMAN RIGHTS COUNCIL, *supra* note 319.

expression, freedom of political association, freedom of the press, freedom from unreasonable search and seizure, freedom to be left alone."[353]

This point is closely related both to the ability to fight tyranny and to the protection of minorities. Akhil Amar has written that "because ballots and the First Amendment have generally worked to prevent full-blown federal tyranny, bullets and the Second Amendment need not bear as much weight today as some pessimists anticipated two centuries ago."[354] However, the fact remains that "[a]lthough the Constitution guarantees a high degree of political freedom and autonomy, 'the Government has often undertaken the secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts on behalf of a hostile foreign power.'"[355] Against such a threat, cryptography allows us to defend our privacy-adjacent rights. This is made clear by the number of constitutional arguments one can make against regulating encryption.[356] Interpreting "arms" to include cryptography would thus sync the first four amendments into a positive feedback loop of privacy protection. Indeed, the Ninth Circuit recognized as much when it struck down export restrictions on cryptography in *Bernstein IV*.[357] That Court concluded that:

> [g]overnment efforts to control encryption . . . may well implicate not only the First Amendment rights of cryptographers . . . but also the constitutional rights of each of us as potential recipients of encryption's bounty. . . . the government's efforts to retard progress in cryptography may implicate the Fourth Amendment, as well as the right to speak anonymously, the right against compelled speech, and the right to informational privacy . . ."[358]

V. Is Cryptography an Arm Protected By the Second Amendment?

The right to bear arms, like all of the other constitutional rights, is not absolute.[359] It does not enshrine "a right to keep and carry any weapon whatsoever . . ."[360] So if we accept that — in light of the ambiguous text but

353. SINGH, *supra* note 9, at 296.

354. Amar, *supra* note 118, at 896.

355. Froomkin, *supra* note 12, at 732 (quoting S. REP. NO. 755, 94th Cong., 2d Sess., pt. 2, at 5 (1976)).

356. *See id.* at 810–46 (exploring the First, Fourth, and Fifth Amendment and generalized privacy right implications of escrowed encryption).

357. *Bernstein IV*, 176 F.3d at 1145–46.

358. *Bernstein IV*, 176 F.3d at 1146 (citations omitted).

359. *See Heller,* 554 U.S. at 626.

360. *Id*. at 626.

powerful purposive arguments — cryptography is an arm, we still must ask if it is an arm protected by the Second Amendment. While answering the first question is difficult, answering the second is not: if cryptography is an "arm," it is clearly one protected by the Second Amendment.

A. In Common Use

Heller tells us that protected weapons are those "'in common use at the time' for lawful purposes like self-defense."[361] As we have seen, this is the glue that connects the operative clause to the prefatory clause: The weapons people kept at home "for lawful purposes like self-defense" were the same ones that they grabbed when rushing to defend their Free State in their role as Militia members.[362] So, we must first ask if cryptography is such a weapon.

"[W]hat line separates 'common' from 'uncommon' ownership is something the Court did not say."[363] However, the Court did give us a benchmark: handguns are common.[364] In fact, the Court claimed that handguns are the most popular weapons for self-defense in our country.[365] That is incorrect. Cryptography is the most common weapon Americans use for self-defense.

Estimates of gun ownership in America vary, but even according the higher estimates, fewer than half of American adults own firearms of any sort.[366] And only about half of those keep their firearms for protection.[367] Meanwhile, fully half of all American adults bank online;[368] all of them protect themselves with Cryptography.[369] Thus, cryptography must qualify as "in common use." And that is before we even consider any of the other uses of cryptography. Anyone who uses Apple's popular iMessage or FaceTime applications is using cryptography to keep his or her communications private.[370] Anyone who uses https to browse the web uses

361. *Id.* at 624 (quoting *Miller*, 307 U.S. at 179). The Court has since made clear that "at the time" refers to the present day. *Caetano v. Massachusetts*, 136 S.Ct. 1027, 1027–28 (2016).

362. *See Heller*, 554 U.S. at 625.

363. *Friedman,* 784 F.3d at 409.

364. *See Heller,* 554 U.S. at 629.

365. *Id.*

366. Gallup, *Guns,* http://www.gallup.com/poll/1645/guns.aspx (last visited May 3, 2015).

367. *See* PEW RESEARCH CENTER, *Why own a gun? Protection is now top reason*, (Mar. 12, 2013), http://www.people-press.org/2013/03/12/why-own-a-gun-protection-is-now-top-reason/.

368. *See* PEW RESEARCH CENTER, *51% of American Adults Bank Online*, (Aug. 7, 2013), http://www.pewinternet.org/2013/08/07/51-of-u-s-adults-bank-online/.

369. *See* DIFFIE & LANDAU, *supra* note 17, at 47-48.

370. *See* SOGHOIAN, *supra* note 265.

cryptography to keep their web viewing habits secret.[371] About one third of web traffic is encrypted in some format.[372] Anyone who takes cash out of an ATM or electronically transfers funds relies on cryptography.[373] As does anyone who uses a virtual private network ("VPN") to remotely access an organization's network.[374] Indeed, cryptography "is an essential basis for trust on the Internet" that facilitates commerce and communication online.[375] It is omnipresent in our day-to-day lives, and it is there for our protection.[376]

We generally use cryptography to protect us financially, from threats like identity theft. One might argue that therein lies a distinction of constitutional import: handguns can be used to protect life and limb, while cryptography is only used to protect property. But that is irrelevant. The *Heller* Court explicitly stated that the "right to self-defense" includes the defense of property.[377] This follows from the common law of self-defense, which treats the difference between defending life and defending property as one of degree rather than of kind.[378] Furthermore, cryptography does in fact protect life and limb, as "at the higher end of the harm's scale, privacy concerns morph into matters of personal security."[379] For example, Somali pirates have begun infiltrating the networks of shipping companies in order to determine which ships they should target.[380] For the sailors on those ships information security is integral to physical security. Another powerful example, domestic violence survivors use cryptography to ensure physical security.[381] Moreover, cyber-attacks can cause physical harm. For example, hackers can disable a car's breaks, or destroy centrifuges.

371. *See id.*

372. Sandvine, *Global Internet Phenomena Spotlight: Encrypted Internet Traffic*, 3, https://www.sandvine.com/downloads/general/global-internet-phenomena/2015/encrypted-internet-traffic.pdf (last visited Nov. 25, 2015).

373. FROOMKIN, *supra* note 12, at 720.

374. SWIRE & AHMAD, *supra* note 254, at 453–54.

375. CLARKE ET AL., *supra* note 171, at 216–17.

376. *See id.*; SWIRE & AHMAD, *supra* note 254, at 453–54.

377. *Heller,* 554 U.S. at 628 ("[T]he inherent right of self-defense has been central to the Second Amendment right. The handgun ban amounts to a prohibition of an entire class of 'arms' that is overwhelmingly chosen by American society for that lawful purpose. The prohibition extends, moreover, to the home, where the need for defense of self, family, *and property* is most acute." (emphasis added)).

378. *See, e.g.*, *Self-Defense,* BLACK'S LAW DICTIONARY (9th ed. 2009) (defining "self-defense" as "The use of force to protect oneself, one's family, or one's *property* from a real or threatened attack." (emphasis added); MODEL PENAL CODE § 3.06.

379. WITTES & BLUM, *supra* note 210, at 138.

380. Patrick Gray, *Risky Business # 401—Deserialization attacks are kind of a big deal,* (Mar. 3, 2016), http://risky.biz/RB401.

381. *See* LAWRENCE, *supra* note 75.

B. Dangerous and Unusual

A related inquiry that some courts undertake is whether the arm at issue is "dangerous and unusual," as such weapons have long been banned and thus fall outside the scope of the Second Amendment.[382] In many ways this is an identical exercise to the previous question, as any weapon "in common use" is, by definition, not "unusual."[383] But the Connecticut Supreme Court, for example, leaned on the fact that knives are less dangerous than handguns in cementing its conclusion that the Second Amendment protects them.[384] Cryptography is unusual here because, unlike most other arms, it is not dangerous.

"An object is 'dangerous' when it is 'likely to cause serious bodily harm.'"[385] Generally, the common law distinguished between weapons that were dangerous per se (e.g., "firearms, daggers, stilettos, and brass knuckles"), and those that were not (e.g., "pocket knives, razors, hammers, wrenches, and cutting tools") based on whether they were primarily designed as weapons or as tools.[386] Cryptography was designed as a weapon, which would normally make it dangerous per se.[387] However, a dangerous weapon is "'an instrumentality designed and constructed to produce death or great bodily harm' and 'for the purpose of bodily assault or defense.'"[388] Obviously, cryptography does not fit this definition. It does not cause bodily injury; it does not kill. Thus, cryptography is an "unusually safe" weapon, which only further supports the conclusion that cryptography is an arm protected by the Second Amendment.[389]

C. Appropriate to a Militia

Lastly, some courts have asked whether the weapon at issue is "appropriate to a militia"[390] or has "some reasonable relationship to the preservation or efficiency of a well regulated militia."[391] If we focus on this

382. *Heller,* 554 U.S. at 627 (citing sources); *see also DeCiccio*, 105 A.3d at 193.

383. *See Friedman,* 784 F.3d at 409; *United States v. Fincher*, 538 F.3d 868, 873–74 (8th Cir. 2008).

384. *DeCiccio*, 105 A.3d at 193.

385. *United States v. Henry,* 688 F.3d 637, 640 (9th Cir. 2012).

386. *Caetano,* 26 N.E.3d at 692.

387. *Id.* (quoting *Commonwealth v. Appleby*, 380 Mass. 296, 303 (1980)).

388. *See id.*

389. *See* VOLOKH, *supra* note 176, at 1482–83 (2009).

390. *See Caetano,* 26 N.E.3d at 694.

391. *Friedman*, 784 F.3d at 410 (citing *Heller*, 554 U.S. at 622–25; *Miller*, 307 U.S. at 178–79). It is not clear this is an appropriate inquiry, given that *Heller* apparently rejected the similar inquiry of whether the weapon at issue was one "usually employed in civilized warfare." Volokh, *supra* note 176, at 219.

question, it seems clear that cryptography should be a protected arm. Those weapons "commonly used for military and police functions" inherently "bear a relation to the preservation and effectiveness of state militias."[392] As explained above, civilized warfare and the military were the primary uses of cryptography for most of its history. Indeed, the NSA, the U.S. Government's main cryptographic agency is part of the Department of Defense and the Director of the NSA is also Commander of U.S. Cyber Command.[393] Furthermore, the types of cryptography we use for self-defense are no longer dramatically different from the types of cryptography used by militaries.[394] Thus, even if the Second Amendment's protections extend only to arms useful in warfare, those protections would still apply to cryptography.

It seems clear that cryptography should be viewed as an arm protected by the Second Amendment. Therefore, we next look at whether the regulations of cryptography being proposed would burden the Second Amendment right.

VI. Would Suggested Regulations Burden the Second Amendment Right?

Of course, concluding that cryptography is an arm that is protected by the Second Amendment does not necessarily foreclose its regulation.[395] Although there are no concrete regulations to evaluate, it is worth thinking about how future regulations would be evaluated, and thus the constitutional considerations policy makers should take into account.

In the years since *Heller* and *McDonald* were decided, the Courts of Appeals have largely coalesced around a two-step test for determining whether laws run afoul of the Second Amendment.[396] At the first step, courts

392. *Friedman*, 784 F.3d at 410

393. CLARKE, ET AL., *supra* note 171, at 185–86.

394. *See id.*; SOGHOIAN *supra* note 265.

395. Few gun laws have been struck down post-*Heller*. *See Tyler v. Hillsdale Cnty. Sheriff's Dept.*, 775 F.3d 308, 334 (6th Cir. 2014) (vacated pending rehearing *en banc*) ("It may be true that no other appeals court has sustained a Second Amendment challenge to a federal firearms regulation since Heller was decided." (citing *United States v. Mahin*, 668 F.3d 119, 123 (4th Cir. 2012); *United States v. Seay*, 620 F.3d 919, 924 (8th Cir. 2010)).

396. *See N.Y. State Rifle & Pistol Ass'n, Inc. v. Cuomo*, 804 F.3d 242, 254 (2d Cir. 2015) (noting that the Second Circuit's two-step approach "broadly comports with the prevailing two-step approach of other courts, including the Third, Fourth, Fifth, Sixth, Seventh, Ninth, Tenth, Eleventh, and D.C. Circuits" and citing *GeorgiaCarry.Org, Inc.* v. *U.S. Army Corps of Eng'rs*, 788 F.3d 1318, 1322 (11th Cir. 2015); *United States v. Chovan*, 735 F.3d 1127, 1136 (9th Cir. 2013); *Nat'l Rifle Ass'n of Am., Inc. v. Bureau of Alcohol, Tobacco, Firearms & Explosives*, 700 F.3d 185, 194 (5th Cir.2012); *United States v. Greeno*, 679 F.3d 510, 518 (6th Cir. 2012); *Heller II*, 670 F.3d at 1252; *Ezell v. City of Chicago*, 651 F.3d 684, 702–03 (7th Cir. 2011); *United States v. Chester*,

"consider whether the restriction burdens conduct protected by the Second Amendment."[397] If the answer is no, the inquiry is over.[398] If the answer is yes, courts proceed to step two, in which they "must determine and apply the appropriate level of scrutiny."[399]

A. Step One

We have already done much of the work required by the first step: determining whether cryptography is a protected arm.[400] However, there are some additional questions to ask. Most importantly, do the sorts of regulations that have been discussed actually burden the Second Amendment right? The cryptography debate has generally not included calls for outright bans on cryptography. Rather, as we have seen, it has centered on requiring companies to include "backdoors."[401]

The White House has studied two slightly different potential back-doors schemes.[402] Under one, the government would retain keys to smartphone encryption.[403] Under the other, the smartphone operating system manufacturer (i.e., Apple or Google) and the government would each retain a part of a key, so that only together would they be capable of decrypting the contents of the phone.[404] These systems and others that may be put forward, like Clipper, accomplish the same end: they "provide some form of access to plaintext outside of the normal channel of encryption or decryption."[405] Such systems may be called "key recovery," "key escrow," "trusted third-party," "exceptional access," "data recovery,"[406] "split key" or "secret sharing."[407] While they "work in a variety of way . . . . [a]ll these systems

628 F.3d 673, 680 (4th Cir. 2010); *United States v. Reese*, 627 F.3d 792, 800–01 (10th Cir. 2010); *United States v. Marzzarella*, 614 F.3d 85, 89 (3d Cir. 2010)).

397. *See id.*

398. *See id.*

399. *See id.*

400. *See id.* at 254–55.

401. TIMBERG, *supra* note 99; WATT, ET AL., *supra* note 101; COMEY, *supra* note 95; Reed, *supra* note 100.

402. Kevin Schaul, *Encryption techniques and the access they give*, WASH. POST, Apr. 10, 2015, *available at* http://apps.washingtonpost.com/g/page/world/encryption-techniques-and-the-access-they-give/1665/ (last accessed Apr. 16, 2015).

403. *Id.*

404. *Id.*

405. *Id.*

406. Hal Abelson, et al. "The Risks of Key Recovery, Key Escrow and Trusted Third-Party Encryption," May 27, 1997, *available at* http://academiccommons.columbia.edu/catalog/ac%3A127127 (last accessed Apr. 16, 2015), at 5–6.

407. SCHAUL, *supra* note 402.

share the essential elements that concern us" here,[408] and so for the sake of ease, this paper will refer to all such systems as "backdoors."

A law requiring backdoors would fundamentally degrade the protection cryptography offers. Regulations that make arms less useful impinge the right.[409] Therefore, requirements that cryptography have backdoors would implicate the Second Amendment.

1. The (In)Security of Backdoors

In order to think about regulations requiring backdoors, it is important to understand why they would burden a Second Amendment right. On the issue of backdoors, Director Comey said:

> There is a misconception that building a lawful intercept solution into a system requires a so-called "back door," one that foreign adversaries and hackers may try to exploit. But that isn't true. We aren't seeking a back-door approach. We want to use the front door, with clarity and transparency, and with clear guidance provided by law. We are completely comfortable with court orders and legal process — front doors that provide the evidence and information we need to investigate crime and prevent terrorist attacks.[410]

NSA Director Admiral Rodgers similarly said: "'Backdoor' is not the context I would use, because when I hear the phrase 'backdoor' I think: 'Well this is kind of shady, why wouldn't you want to go in the front door, be very public?'"[411] Director Comey and Admiral Rogers exhibited the same misunderstanding as the Washington Post Editorial Board when it opined that:

408. ABELSON, ET AL., *supra* note 406, at 5–6; *see also Encryption Technology and Possible US Policy Responses: Hearing Before the Info. Tech. Subcomm. of the H. Comm. on Gov. Oversight & Reform, 113th Cong.* (2013) (statement of Matt Blaze, Univ. of Pennsylvania) [hereinafter "Blaze Testimony"].

409. *See Heller*, 554 U.S. at 628–635 (D.C. law mandating trigger locks is unconstitutional); *cf. Kolbe*, 813 F.3d at 175 ("Early American provisions protecting the right to "arms" were also crafted partly in response to British measures that, while not taking away guns entirely, drastically impaired their utility — suggesting 'arms' should be read to protect all those items necessary to use the weapons effectively.") (citing Saul Cornell, *The Early American Origins of the Modern Gun Control Debate: The Right to Bear Arms, Firearms Regulation, and the Lessons of History*, 17 STAN. L. & POL'Y REV. 571, 577 (2006)).

410. COMEY, *supra* note 95.

411. Quoted in Tom McCarthy, *NSA Director Defends Plan to Maintain 'Backdoors' Into Technology Companies,* THE GUARDIAN, Feb. 23, 2015, *available at* http://www.theguardian.com/us-news/2015/feb/23/nsa-director-defends-backdoors-into-technology-companies (last accessed Apr. 22, 2015).

> A police 'back door' for all smartphones is undesirable — a back door can and will be exploited by bad guys, too. However, with all their wizardry, perhaps Apple and Google could invent a kind of secure golden key they would retain and use only when a court has approved a search warrant.[412]

Director Comey and *The Washington Post* are right that backdoors are easily attacked. The problem with their analysis is that there is no technical difference between a "back door," a "front door," or a door locked with a "secure golden key."[413] "Backdoor access is a technical requirement, and limiting access to law enforcement is a policy requirement. As an engineer, [one] cannot design a system that works differently in the presence of a particular badge or a signed piece of paper."[414] Regardless of what we call the door, it comes with the risk of being kicked down, having its locks picked, or their keys stolen. As Bruce Schneier put it, "You can't build a backdoor that only the good guys can walk through."[415]

This is not a theoretical point: "Backdoor access built for the good guys is routinely used by the bad guys."[416] For example, Google built a backdoor into some of its applications, including Gmail, in order to comply with lawful search warrants.[417] "China's hackers subverted the access system Google put in place to comply with U.S. intercept orders."[418] Because Google had created backdoors into Gmail, Chinese hackers were able to spy on Chinese

412. Editorial Board, *Compromise needed on smartphone encryption*, WASH. POST, Oct. 2, 2014, *available at* http://www.washingtonpost.com/opinions/compromise-needed-on-smartphone-encryption/2014/10/03/96680bf8-4a77-11e4-891d-713f052086a0_story.html (last accessed Apr. 16, 2015).

413. *See* Jeffrey Vagle and Matt Blaze, *Security 'Front Doors' vs. 'Back Doors': A Distinction Without a Difference*, JUST SECURITY, Oct. 17, 2014, *available at* http://justsecurity.org/16503/security-front-doors-vs-back-doors-distinction-difference/ (last accessed Apr. 16, 2015) ("[T]he difference between a 'front door' vs. a 'back door' approach to law enforcement intercept of encrypted communications is purely semantic."); *see also* Bruce Schneier, *iPhone Encryption and the Return of the Crypto Wars*, SCHNEIER ON SECURITY, Oct. 6, 2014, *available at* https://www.schneier.com/blog/archives/2014/10/iphone_encrypti_1.html (last accessed Apr. 16, 2015); Bruce Schneier, *Crypto Wars II*, SCHNEIER ON SECURITY, Nov. 15, 2014, *available at* https://www.schneier.com/crypto-gram/archives/2014/1115.html (last accessed Apr.16, 2015); Soghoian, *supra* note 265.

414. Bruce Schneier, quoted in Price, *supra* note 190.

415. Schneier, *iPhone Encryption and the Return of the Crypto Wars*, *supra* note 413.

416. Bruce Schneier, *U.S. enables Chinese hacking of Google,* CNN, Jan. 23, 2010, *available at* http://www.cnn.com/2010/OPINION/01/23/schneier.google.hacking/index.html (last accessed Apr. 23, 2015).

417. *Id*.

418. *Id.*

human rights activists.[419] Similarly, in 2005, an unknown attacker exploited the lawful intercept capabilities that Vodafone and Ericsson built into their cellular infrastructure to eavesdrop on the cell phone calls of the Greek prime minister, defense minister, foreign affairs minister, and a host of other prominent Greek figures.[420] And although not quite of the same genre, encryption that had been weakened to comply with old U.S. export laws was showing up in internet protocols until 2015, rendering about one third of all internet sites vulnerable, including the FBI's own tip reporting site.[421]

This is not a matter of idiosyncratic mistakes being made; backdoors are inherently insecure for several reasons. First, backdoors provide another path to the information being kept secret.[422] The attacker now gets two bites at the apple: rather than having to break or circumvent the encryption on the plaintext, an attacker can break or circumvent *either* the encryption on the plain text or the protections on the key to the plaintext.[423]

Second, and relatedly, implementing a backdoor requires trusting someone to hold and to protect the keys to the back door.[424] Regardless of whether the keys are held by the government or a company,[425] this "represents a universal vulnerability in any escrowed communication system."[426] It opens up the possibility of insider abuse (rogue employees could be paid handsomely for stolen keys) and creates a wonderful target for attackers who could render huge swaths of encryption useless with one successful attack.[427] To make this problem worse, backdoors need to point

419. *See id;* Google, *A new approach to China,* GOOGLE OFFICIAL BLOG, Jan. 12, 2010, *available at* http://googleblog.blogspot.com/2010/01/new-approach-to-china.html (last accessed Apr. 23, 2015).

420. SCHNEIER, *supra* note 416*;* Vassilis Prevelakis & Diomidis Spinellis, *The Athens Affair: How some extremely smart hackers pulled off the most audacious cell-network break-in ever,* IEEE SPECTRUM, June 29, 2007, *available at* http://spectrum.ieee.org/telecom/security/the-athens-affair (last accessed Apr. 23, 2015); Abelson, *supra* note 406*,* at 10 & 17.

421. Matthew Green, *A History of Backdoors,* A FEW THOUGHTS ON CRYPTOGRAPHIC ENGINEERING, July 20, 2015, *available at* http://blog.cryptographyengineering.com/2015/07/a-history-of-backdoors.html (last accessed Nov. 18, 2015).

422. ABELSON, et al., *supra* note 406*,* at 11.

423. *See id.*

424. *Id.,* at 11–12; Matthew Green, *How do we build encryption backdoors?,* SOME THOUGHTS ON CRYPTOGRAPHIC ENGINEERING, Apr. 16, 2015, *available at* http://blog.cryptographyengineering.com/2015/04/how-do-we-build-encryption-backdors.html (last accessed Apr. 22, 2015).

425. ABELSON, ET AL., *supra* note 406*,* at 13.

426. GREEN, *supra* note 424.

427. *See,* ABELSON, ET AL., *supra* note 406, at 11–12; Abelson, et al., *Keys Under Doormats: mandating insecurity by requiring government access to all data and communications*, July 6, 2015, *available at* http://hdl.handle.net/1721.1/97690 (last accessed Aug. 4, 2016), at 2; Green, *supra* note 424.

to the location of their keys, which serves as "a roadmap showing law enforcement how to recover the plaintext, but it may also show unauthorized attackers where to focus their efforts."[428] While there are schemes designed to minimize this risk — for example, by splitting the backdoor key between different escrow agents — these systems invariably introduce their own new vulnerabilities, and increase the financial costs of the system.[429] Additionally, many of those schemes would be incompatible with law enforcement's requirement of rapid access to data.[430] Indeed, the difficulty of protecting escrowed keys is highlighted by the theft from RSA of their "seed keys," from which the keys for their hardware tokens are generated.[431]

Third, and perhaps most importantly, adding backdoors to encryption schemes makes them dramatically more complex, and in computer security, vulnerability increases as complexity increases.[432] "Every additional line of code you add to a system creates the possibility of more bugs."[433] Computer scientists refer to the "attack surface": The more complex the code, the larger the attack surface, and the less secure the system.[434] "[S]ecure cryptographic systems are deceptively hard to design and build properly . . . . Very small changes frequently introduce fatal security flaws."[435] The changes required for implementing backdoors would not be "very small," rather "[t]hese schemes require you to alter every protocol in your encryption system, at a pretty fundamental level."[436] And to make matters worse, the fundamental changes required, "by [their] very nature, [have] to touch the most sensitive parts of the system because the wiretapping interface has to have the raw users' communications going through it, which means that when you have a bug in that interface, it could lead to a catastrophic loss of security of the system."[437] Add these fundamental changes to cryptographic systems that are "already so complex that even normal issues stress them to the breaking point,"

428. ABELSON, ET AL., *supra* note 406, at 12.

429. *Id.* at 12. So called "threshold encryption," which theoretically allows decryption to be done via several keys without bringing them together, may provide a solution to some of these problems, but it has never been implemented in real life. Green, *supra* note 424*; see also,* H.L. Nguyen, *RSA Threshold Cryptography,* May 4, 2005, (unpublished Ph.D. Dissertation, University of Bristol) *available at* https://www.cs.ox.ac.uk/files/269/Thesis.pdf (last accessed Apr. 22, 2015).

430. ABELSON, ET AL., *supra* note 427*,* at 2.

431. *Id.* at 9.

432. *See id.* at 16.

433. SOGHOIAN, *supra* note 265.

434. *Id.*

435. ABELSON, ET AL., *supra* note 406*,* at 13.

436. GREEN, *supra* note 424.

437. SOGHOIAN, *supra* note 265.

and we have a recipe for disaster.[438] Importantly, this is not a simple matter of competence, expertise, or trying harder.[439] Complexity induced problems even plagued the Clipper Chip, designed by the NSA, which "may be the most advanced cryptographic enterprise in the world."[440]

Additionally, some of the best practices in cryptographic engineering for data in motion are simply incompatible with the requirements of building backdoors.[441] The first of these is "forward security."[442] In many systems for transmitting data, the data is first encrypted with a symmetric key — that is, a key which is used both for encrypting and decrypting data — using a different symmetric key for each communication. That symmetric key is then itself encrypted with a public key. Public keys are used to encrypt data so that it can only be decrypted with the corresponding private key. This system works well as long as the relevant private key is never compromised; once it is, however, the attacker can decrypt all of the data sent using the corresponding public key in the past — the attacker simply uses the private key to decrypt the symmetric key, and uses that to decrypt the message.[443] To mitigate this risk, cryptographers prefer systems that provide "forward security." In these systems, the permanent public and private keys are not used to encrypt anything, but are only used to allow the communicating parties to identify each other; once that occurs, disposable keys for one time use are created.[444] Because a new key is used for each transaction, a stolen key only endangers a single communication rather than all previous and future communications.[445] Because the point of a long-term escrow key for law enforcement is to introduce the backwards looking risk that forward security is designed to eliminate, "all known methods of achieving third-party escrow are incompatible with forward security."[446]

Another best practice that key escrow compromises is "authenticated encryption."[447] This technique provides confidentiality while at the same

438. Matthew Green, *Attack of the week: FREAK or ('factoring the NSA for fun and profit'),* A FEW THOUGHTS ON CRYPTOGRAPHIC ENGINEERING, Mar. 3, 2015, *available at* http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-factoring-nsa.html (last accessed Apr. 23, 2015); *see also* Green, *supra* note 424, ("[o]ur encryption software is already so complex that it's literally at the breaking point.").

439. ABELSON, ET AL., *supra* note 406*,* at 13.

440. *Id.*

441. *See* ABELSON, ET AL., *supra* note 427*,* at 2.

442. *Id.*

443. *Id.* at 12.

444. *Id.*

445. *Id.*

446. *Id.*

447. *Id.* at 13.

time confirming whom one is communicating with.[448] In these systems, escrowing keys would give the party with the escrowed key the power, not only to read encrypted communications, but "to forge traffic to the recipient" in such a way that it appears to be coming from the original sender.[449]

"[B]uilding the secure infrastructure of the breathtaking scale and complexity that would be required for such a [backdoor] scheme is beyond the experience and current competency of the field . . . ."[450] While Director Comey and Admiral Rogers apparently disagree with this conclusion, they have not produced any technical explanation for their disagreement.[451] And most, if not all, technical experts agree that that all cryptographic systems with back doors "are inherently less secure" than they would be without backdoors. Therefore, mandating backdoors would surely burden the individual's Second Amendment rights.

2. Presumptively Valid Regulations

In analyzing the constitutionality of an arms regulation, some courts first ask whether the regulations at issue are among those that the Heller court would consider "presumptively lawful."[452] *Heller* stated:

> [N]othing in our opinion should be taken to cast doubt on longstanding prohibitions on the possession of firearms by felons and the mentally ill, or laws forbidding the carrying of firearms in sensitive places such as schools and government buildings, or laws imposing conditions and qualifications on the commercial sale of arms.[453]

There are no longstanding regulations of domestic cryptography, although the few remaining export control restrictions would perhaps count.

Some narrow cryptography regulations might be cognizable as presumptively valid, in keeping with the spirit of the safe harbor. For example, laws prohibiting felons from carrying firearms might have their equivalents in laws prohibiting convicted child pornographers from encrypting their data. However, in order to be analogous to the regulations listed by the court, these hypothetically valid regulations would need to be limited and tailored to situations of particular concern. Forcing companies

448. *Id.*

449. *Id.*

450. ABELSON, ET AL., *supra* note 406, at 19.

451. *See, e.g.,* REED, *supra* note 100, (quoting Adm. Rogers saying "My position is — hey look, I think that we're lying that this isn't technically feasible.").

452. *See, e.g., Chovan*, 735 F.3d at 1137.

453. *Heller*, 554 U.S. at 626–27.

to build backdoors into cryptography, or any other attempt to regulate the mass consumption of cryptography, is of vastly greater scope than the court apparently imagined when stating that it did not want to cast doubt on certain regulations.

3. Do regulations on suppliers infringe on the Second Amendment?

The last of *Heller*'s enumerated exceptions brings us to another point. Most of the public discussion about cryptography controls has focused on regulating companies — such as Apple and Google — that manufacture consumer electronics, rather than on regulating the individual user of cryptography. Whether, and to what extent, those who trade in arms have Second Amendment rights (and whether and to what extent regulations on them burden the Second Amendment rights of their customers) is still being hashed out in the lower courts. [454] While a full analysis of these issues is beyond the scope of this paper, it appears the weight of precedent supports the conclusion that manufacturers, retailers, and others either have their own Second Amendment rights or can sue to enforce the Second Amendment rights of their customers.[455] If manufacturers, retailers, and other arms related businesses have Second Amendment rights (or can enforce those of their customers), the fact that cryptography regulations act on Apple and Google rather than individuals would be constitutionally irrelevant.

Eugene Volokh has suggested that the proper way to evaluate whether restrictions on manufacturers and retailers violate the Second Amendment might be to ask whether those restrictions "impose a substantial burden on the exercise of the protected right."[456] That is to say that restrictions that make protected weapons "substantially costlier or harder to get" would be unconstitutional.[457] This approach would similarly make it irrelevant whether the sort of regulations being considered act on retailers rather than consumers.

454. *See generally* David B. Kopel, *Does the Second Amendment Protect Firearms Commerce?,* 127 HARV. L. REV. 230 (Apr. 11, 2014).

455. *See, e.g., Marzzarella*, 614 F.3d at 92 n. 8; *Ezell v. City of Chicago*, 651 F.3d 684, 711 (7th Cir. 2011); *Kole v. Village of Norridge*, 941 F. Supp. 2d 933, 945 (N.D. Ill. 2013); *Ill. Ass'n of Firearms Retailers v. City of Chicago*, 961 F. Supp. 2d 928, 931 n. 3 (N.D. Ill. 2014); *but see United States v. Chafin*, 423 F. App'x 342, 344 (4th Cir. 2011); *United States v. Conrad*, 923 F. Supp. 2d 843, 852 (W.D. Va. 2013).

456. VOLOKH, *supra* note 176, at 1545.

457. *Id.*

B. Step Two

At the second step of the analysis, most courts identify an appropriate level of scrutiny and apply it to the regulation.[458] Drawing on First Amendment doctrine, many of the Circuits use a sliding scale of judicial scrutiny depending on how severe a burden the regulation places on the Second Amendment right and "how close the law comes to the core of the Second Amendment right."[459] Of the three traditional levels of scrutiny — rational basis, intermediate, and strict — *Heller* did rule out rational basis.[460] This leaves a choice between intermediate and strict scrutiny (as well as points on the opaque continuum between them) on the table for courts to choose from.[461] And that choice is a difficult and contentious one.[462]

In most cases, the Circuits have ended up applying some form of intermediate scrutiny.[463] Yet many courts have indicated that strict scrutiny would be appropriate for those cases which burden the "core" of the right: the "right of law-abiding, responsible citizens to use arms in defense of hearth and home."[464] There are also those judges who believe strict scrutiny should always apply.[465]

However, some restrictions — those that "destroy" rather than merely burden that right — are per se invalidated, without the application of any level of scrutiny, as was the D.C. law in *Heller*.[466] An outright ban on all cryptography would likely fall into that category. In *Heller*, the Court held that the D.C. law, which banned handgun possession in the home was

458. *See, e.g.*, *N.Y. State Rifle & Pistol Ass'n*, 904 F.3d at 55–59.

459. *Chovan*, 735 F.3d at 1138; *see e.g.*, *N.Y. State Rifle & Pistol Ass'n*, 804 F.3d at 258–60; *Marzarella*, 614 F.3d at 97; *NRA v. ATF*, 700 F.3d 185, 195 (5th Cir. 2012); *Ezell*, 651 F.3d at 707; *Peruta*, 742 F.3d at 1168 n.15.

460. *Heller*, 554 U.S. at 628 n. 27.

461. *See Tyler*, 775 F.3d at 323 ("intermediate and strict scrutiny are not binary poles in the area of heightened scrutiny. These familiar tests can take on many names and versions").

462. *See id.* ("The appropriate level of scrutiny that courts should apply in Second Amendment cases . . . remains a difficult, highly contested question.").

463. *See Tyler*, 775 F.3d at 324–26 (collecting cases).

464. *See Kachalsky v. County of Westchester*, 701 F.3d 81, 93–94 (2d Cir. 2012) (quoting *Heller*, 554 U.S. at 93–94); *United States v. Masciandaro*, 638 F.3d 458, 471 (4th Cir. 2011) ("we find the application of strict scrutiny important to protect the core right of the self-defense of a law-abiding citizen in his home"); *see also Peruta*, 742 F.3d at 1168 n.15.

465. *See Tyler*, 775 F.3d at 328 ("[W]e prefer strict scrutiny over intermediate scrutiny. In choosing strict scrutiny, we join a significant, increasingly emergent though, as yet, minority view . . . ." (citing *Chovan*, 735 F.3d at 1145–46, 1149–52 (Bea, J., concurring); *NRA v. ATF*, 714 F.3d 334, 336 (5th Cir.2013) (Jones, J., dissental, joined by Jolly, Smith, Clement, Owen, & Elrod, JJ.); *Heller II*, 670 F.3d at 1284 (Kavanaugh, J., dissenting).

466. *See Heller*, 554 U.S. at 628; *Peruta*, 742 F.3d 1170.

unconstitutional.[467] The Court wrote that, "[u]nder any of the standards of scrutiny . . . banning from the home the most preferred firearm in the nation to keep and use for protection of one's home and family would fail constitutional muster."[468] By that logic, banning cryptography — which is more commonly used for self-defense than handguns — would surely violate the Second Amendment, under any standard of scrutiny.

But backdoor mandates could fall into that category as well. One way to think about a regulation mandating backdoors is as a ban on encryption products without backdoors. Thought of, in this way, such regulations might be akin to the handgun ban struck down in *Heller*. After all, the law in *Heller* did not ban all guns. The Court wrote:

> It is no answer to say, as petitioners do, that it is permissible to ban the possession of handguns so long as the possession of other firearms (i.e., long guns) is allowed. It is enough to note, as we have observed, that the American people have considered the handgun to be the quintessential self-defense weapon. There are many reasons that a citizen may prefer a handgun for home defense: It is easier to store in a location that is readily accessible in an emergency; it cannot easily be redirected or wrestled away by an attacker; it is easier to use for those without the upper-body strength to lift and aim a long gun; it can be pointed at a burglar with one hand while the other hand dials the police. Whatever the reason, handguns are the most popular weapon chosen by Americans for self-defense in the home, and a complete prohibition of their use is invalid.[469]

Similar logic could apply here, as unbackdoored cryptography is the industry standard and there are good reasons to prefer it.[470]

But even if per se invalidation is not appropriate, strict scrutiny of a general back-door requirement may well be. Courts have indicated that strict scrutiny is applicable in the Second Amendment context to regulations,

467. *Heller*, 554 U.S. at 635.

468. *Id.* at 628–29.

469. *Id.* at 629.

470. Public consciousness has obviously not coalesced around unbackdoored encryption in the same way it has around the handgun as "the quintessential self-defense weapon." But it seems unlikely that the popular imagination of self-defense was intended to be a deciding factor in the Court's analysis allowing per se invalidation. Constitutional interpretation does not generally hinge on Clint Eastwood's prop choices. And, in any event, unbackdoored encryption is likely at least as popular as handguns for self-defense. *See Kolbe*, 813 F.3d at 181 ("A semi-automatic rifle may not be 'the quintessential self-defense weapon,' as *Heller* described the handgun; nonetheless, as we explained previously, AR–15s and the like are commonly possessed by law-abiding citizens for self-defense and other lawful purposes and are protected under the Second Amendment.") (citation omitted)).

which put a severe burden on the core of the right.[471] Serious degradation of the usefulness of encryption would likely fit this standard.

To begin with, the burden would be severe. Let's continue to think about a law mandating backdoors as law that outlaws a narrower class of arms: encryption without back doors. Such a regulation would be "a complete prohibition" on a class of arms, rather than something that "merely regulate[s] the manner in which persons may exercise their Second Amendment rights."[472] Courts have indicated that a ban on an entire class of arms is a severe Second Amendment burden.[473]

Backdoors also simply make encryption far less effective.[474] Moreover, such regulations would not leave adequate alternative means for self-defense available.[475] This is different from the firearm context: While a rational citizen might have good reasons to choose a handgun over a semiautomatic weapon for self-defense in the home,[476] or vise-versa,[477] there are few reasons to prefer encryption without a backdoor.[478] And what reasons there are — for example, enabling you to retrieve information if you lose a password — are unrelated to the effectiveness of the weapon for self-defense.

But not all laws putting a severe burden on the Second Amendment right trigger strict scrutiny. They only do so if they impinge upon the "core" of that right: the right to self-defense in the home.[479] Banning encryption without backdoors would impinge on that core, because it would implicate the privacy and security that we associate with our homes.[480] Therefore, strict scrutiny should probably apply.

However, that still leaves the issue of applying the chosen standard. Although the standards of scrutiny are imprecise,[481] both strict and intermediate scrutiny requires weighing the importance of the government interest being protected by a regulation and the degree of fit between the regulation and that interest. Strict scrutiny, famously, is "'strict' in theory but usually 'fatal' in fact."[482] It places the burden on the government to show

471. *See, e.g.*, *Kolbe*, 813 F.3d at 181; *N.Y. Rifle & Pistol Ass'n*, 805 F.3d at 259.
472. *N.Y. Rifle & Pistol Ass'n*, 805 F.3d at 259; *see also Kolbe*, 813 F.3d at 179–84.
473. *Id.*
474. See *Heller*, 554 U.S. at 628–635; *cf. Kolbe*, 813 F.3d at 175.
475. *See N.Y. Rifle & Pistol Ass'n*, 805 F.3d at 259; *Kolbe*, 813 F.3d at 180–81.
476. *See Heller*, 554 U.S. at 629.
477. *See Friedman*, 784 F.3d at 411.
478. *See supra* section VI.A.1.
479. *See N.Y. Rifle & Pistol Ass'n*, 805 F.3d at 259.
480. *See supra* section IV.B.5.
481. *See, e.g.*, *Tyler*, 775 F.3d at 322–23.
482. *Bernal v. Fainter*, 467 U.S. 216, 219 n. 6 (1984).

that a law is "narrowly tailored to serve a compelling state interest."[483] By contrast, intermediate scrutiny "require[s] the asserted governmental end to be more than just legitimate, either 'significant,' 'substantial,' or 'important'" and "require[s] the fit between the challenged regulation and the asserted objective be reasonable, not perfect."[484]

In terms of the importance of the government interest at stake, the choice between standards is irrelevant: public safety and crime prevention — presumably the goal of any regulation on cryptography — is the ultimate government interest.[485] But the choice between intermediate and strict scrutiny is likely to impact the analysis of the fit between the law and the government interest.

However, under either standard a general backdoor mandate may be troublesome, for it would affect the vast majority of Americans in their everyday lives in order to solve a problem that only occurs relatively rarely. Perhaps "this is to burn the house to roast the pig,"[486] rather than a reasonably or narrowly tailored solution.

Under intermediate scrutiny, many courts have upheld firearms regulations in the face of Second Amendment challenges because they gave substantial deference to the legislature's judgment about the necessity of the law at issue.[487] Whether the deference those Courts give to the legislature is appropriate is beyond the scope of this article.[488] The important point is that if cryptography regulations were enacted, that deference alone may, in practice, be enough to uphold them.

However, Courts often draw on the more developed First Amendment doctrine when dealing with Second Amendment cases.[489] Traditionally in the First Amendment context, intermediate scrutiny requires that a regulation not burden substantially more of the right than necessary to achieve the government interest.[490] Meeting that standard may be difficult for a regulation requiring

483. *FEC v. Wis. Right to Life, Inc.*, 551 U.S. 449, 465 (2007); *United States v. Playboy Entm't Grp.*, 529 U.S. 803, 817 (2000).

484. *Marzzarella*, 614 F.3d at 97–98 (collecting cases).

485. *See Heller*, 554 U.S. at 689 (Breyer, J., dissenting) (public safety is "a primary concern of every government" (quoting *United States v. Salerno*, 481 U.S. 739, 755 (1987))); *see also Dearth v. Lynch*, 791 F.3d 32, 45 (D.C. Cir. 2015) ("The Government's interest in preventing crime is not merely substantial and important; it is 'compelling.'").

486. *Butler v. State of Mich.*, 352 U.S. 380 (1957).

487. *See Drake*, 724 F.3d at 436–37; *Woollard*, 712 F.3d at 881; *Kachalsky*, 701 F.3d at 97.

488. *See Peruta*, 742 F.3d 1177.

489. *See*, *e.g.*, *Tyler*, 775 F.3d at 327 n.14.

490. *See Turner Broadcasting System, Inc. v. F.C.C.*, 512 U.S. 622, 662 (1994); *Ward v. Rock Against Racism*, 491 U.S. 781, 799 (1989).

backdoors, which would impact most Americans, the vast majority of whom are law abiding citizens practicing legitimate self-defense.[491]

Another factor that should be considered in determining whether such regulation is appropriately tailored are how many alternative routes of surveillance and information gathering the government has, and how effective those routes are,[492] as well as how few instances there have been of cryptography foiling law enforcement.[493] Furthermore, even though public safety and crime prevention is a compelling state interest, cryptography regulations have a more attenuated relationship to that interest than firearms regulations.

II. Conclusion

The Second Amendment should not be confined to relevance in the analog world any more than the First or Fourth Amendments. In the digital world, we live in the shadow of online threats to our property, our safety, and our liberty. In this world, the primary tool with which we can defend ourselves is cryptography. Thus, because the Second Amendment has as its ultimate aim enabling us to defend ourselves — be it against criminals or tyrants — that Amendment should protect cryptography.

491. *Cf. Peruta*, 742 F.3d at 1176–78.

492. *See e.g.*, Urs Grasser, et al., *Don't Panic: Making Progress on the "Going Dark" Debate*, Feb. 1, 2016, *available at* https://cyber.law.harvard.edu/pubrelease/dont-panic/ (last accessed Feb. 4, 2016).

493. *See e.g.*, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety,* Nov. 2015, *available at* http://manhattanda.org/sites/default/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety.pdf (last accessed Feb. 4, 2016) (noting 111 instances between Sept. 2014 and Oct. 2015 in which search warrants could not be executed because of encryption but not claiming that in any case it prevented prosecution).