The Right to Data Encryption

STEVEN W SCHLESINGER*
DR. SHLOMIT YANISKY-RAVID**

TABLE OF CONTENTS

 Research Fellow at the Shalom Comparative Research Institute, Eliyahu Law & Tech Center; Kelley Drye & Warren LLP; Ordained Rabbi; JD Fordham University School of Law. I would like to thank my incredible wife Hannah and the rest of my family for supporting and enabling me to pursue a career in the field of law.

 Professor of Law, PhD; Visiting Professor, Fordham University School of Law; Head of the IP-AI & Blockchain Research Project, Fordham Law Center on Law and Information Policy (CLIP); Professor Fellow, Yale Law School, Information Society Project (ISP); Professor of Law, Ono Academic College, Law School (OAC), Israel; Founder and Academic Director, the Shalom Comparative Research Institute, Eliyahu Law & Tech Center, OAC, Israel. I would like to thank Dean Matthew Diller, Dean of the Fordham Law School; the late Professor Joel Reidenberg, the Founder of CLIP; Dean Elad Finkelstein, Dean of OAC Law School; Professor Jack Balkin, Yale Law School, the Founder and Director of Yale Law School, ISP; and to the ISP Fellows for their support and contribution to this Article. Special thanks to Ms. Judy Arad for her outstanding and devoted work. We would like to also thank Emily Kawahara for her time and invaluable editorial input.

I. INTRODUCTION

> *"[I]f you want to keep a secret you must also hide it from yourself. You must know all the while that it is there, but until it is needed you must never let it emerge . . . ."*[1]

Facebook's plans to integrate and encrypt its messaging services across Messenger, Instagram, and WhatsApp faced a governmental objection.[2] In an open letter, then-Attorney General William Barr asked Facebook to

1. GEORGE ORWELL, NINETEEN EIGHTY-FOUR 294 (Alfred A. Knopf, Inc. 1992) (1949).

2. Lauren Feiner, *Here is AG Barr's Full Letter to Facebook Asking it Not to Make Messages Completely Secret*, CNBC (Oct. 4, 2019, 9:19 AM), https://www.cnbc.com/2019/10/03/ag-barr-will-reportedly-ask-facebook-to-postpone-encrypted-messaging-plans.html [https://perma.cc/6ZGD-TQ77]. In October 2021, Facebook changed its company name to Meta. *See, e.g.*, Salvador Rodriguez, *Facebook Changes Company Name to Meta*, CNBC (Oct. 28, 2021, 2:18 PM), https://www.cnbc.com/2021/10/28/facebook-changes-company-name-to-meta.html [https://perma.cc/AAJ2-WRXP].

postpone encryption plans, calling on them to create a way for law enforcement to access personal user data when searching for illegal content.[3] The letter stated that "[s]ecurity enhancements to the virtual world should not make us more vulnerable in the physical world. . . . Companies should not deliberately design their systems to preclude any form of access to content, even for preventing or investigating the most serious crimes."[4]

Facebook's response illuminates a different perspective that will be the focus of this Article. Facebook believes that people have the right to private online conversations, wherever they are in the world and, therefore, strongly opposes governmental attempts to build backdoors because such attempts would undermine the privacy and security of people everywhere. Digital information use is nearing ubiquity and it is now more important than ever to ensure its protection.[5] Individuals should have the right to defend their data with the same vigor and rights afforded to physical property.

This Article posits that digital information is of equal importance to tangible assets, if not more so. However, because existing legal regimes fail to address this need aptly, legislators must establish a system in which citizens may encrypt their digital information without legal hindrance. Data encryption opponents' fear that personal data encryption would, at least in some respects, hamper the United States government's ability to unveil and combat criminal and illegal conduct or terrorist threats that risk public safety.[6] Still, this Article suggests that the right to data encryption is vital to personal liberty, and for protecting privacy and legitimate commercial interests, especially in the modern technological age.

Technology users in the United States can utilize versatile, accessible, and formidable encryption methods to defend their data. However, the government seeks to prevent citizens from doing so.[7] While balancing

3. *Id.*
4. *Id.*
5. *See* John Mylan Traylor, Note, *Shedding Light on the "Going Dark" Problem and the Encryption Debate*, 50 U. MICH. J.L. REFORM 489, 489–90 (2017).
6. If the average citizen adopts strong encryption, which is quickly becoming a reality, law enforcement will face challenges when trying to access protected data, even with the court's assistance. *See* Wei Chen Lin, Comment, *Where Are Your Papers?: The Fourth Amendment, the Stored Communications Act, the Third-Party Doctrine, the Cloud, and Encryption*, 65 DEPAUL L. REV. 1093, 1131 (2016) (discussing the government's attempts to outright ban encryption). Law enforcement might be able to kick down one's door in an emergency, but breaking strong encryption is a nigh-impossible task. *Id.* at 1127.
7. Or at least implement "backdoor" routes for government access to encrypted data. *See* Riana Pfefferkorn, *Everything Radiates: Does the Fourth Amendment Regulate*

governmental objectives with private and commercial liberties is essential, society's outlook has changed in recent years. Society is as—or more—concerned with the government's power and control over personal data as with security and protection from foreign and domestic attacks.[8] To this end, there is a clear need for a legal framework to address the parity between the right to encryption and governmental access.

While society's dependence on data and technology emerges, the lack of adequate legal protection has become a significant impediment. Using several non-United States jurisdictions to illustrate alternative methods, it is clear that the United States should acknowledge the right to data privacy and accommodate the growing need for equitable data encryption.

Thus, this Article suggests a new right: The Right to Data Encryption.

Part II recounts a brief history of encryption; understanding the crux of this issue necessitates familiarity with encryption's storied past and its rise to near-ubiquitous use. Part II also discusses various ways encryption is now integral to daily life within our society. Next, Part III discusses why our society needs encryption, introduces various encryption terms and concepts, and presents several accessible encryption tools and platforms that users now employ. This Part also surveys encryption technology in a broad and readily understandable fashion. Part IV discusses different attempts to either quash or bolster data encryption and privacy rights in the United States. This Part focuses on governmental interests in having a digital key to overcome data encryption tools and discusses the implications of the Fourth and Fifth Amendments on data encryption. Part V then addresses several proposed alternative resolutions to data security and culminates with the right to data encryption, its exceptions, and potential drawbacks. Part VI provides several theoretical justifications to illuminate why the right to encryption is the preferred solution, despite potential difficulties. Part VII concludes that a right to data encryption is imperative for societal privacy going forward, while still considering the features and exceptions involved with such a right.

Side-Channel Cryptanalysis?, 49 CONN. L. REV. 1393, 1403 (2017) (citing STEVEN LEVY, CRYPTO: HOW THE CODE REBELS BEAT THE GOVERNMENT—SAVING PRIVACY IN THE DIGITAL AGE 13–15 (2001)) (noting that until recently the government jealously guarded encryption methods).

8. *See generally* Lin, *supra* note 6 (discussing the need for encryption in the technology age and that people prefer to protect their data rather than allow unfettered governmental access regardless of government's proposed justifications).

II. BACKGROUND: THE HISTORICAL PERSPECTIVE

A. A History of Encryption

Encryption is nothing new to society; historians have discovered widespread use of encryption methods dating as far back as the eighth century.[9] While encryption methods or techniques to obfuscate and protect one's information were often used in a military context, the general idea of encrypting one's data was historically necessary and remains essential.[10] Eventually, the advent of advanced computing gave rise to a new type of protection: Digital Encryption.[11]

In the mid-1900s, militaries developed hardware-based encryptions[12] to protect and access sensitive information from foreign intelligence entities.[13] It was then that the United States government's interest in controlling encryption technology increased.[14] Eventually, the world entered the

9. Some Ancient Greeks would tattoo messages upon their slave's head, let the hair grow back, then send the slave to a recipient so they could shave the slave's head and read the message. Michael Wachtel, Note, *Give Me Your Password Because Congress Can Say So: An Analysis of Fifth Amendment Protection Afforded Individuals Regarding Compelled Production of Encrypted Data and Possible Solutions to the Problem of Getting Data from Someone's Mind*, 14 U. PITT. J. TECH. L. POL'Y 44, 47 (2013) (quoting Brendan M. Palfreyman, Note, *Lessons from the British and American Approaches to Compelled Decryption*, 75 BROOK. L. REV. 345, 349 (2009)); *see also* Daniel J. Sherwinter, Comment, *Surveillance's Slippery Slope: Using Encryption to Recapture Privacy Rights*, 5 J. TELECOMM & HIGH TECH L. 501, 512–13 (2007).

10. *See* Sherwinter, *supra* note 9.

11. *Id.* at 513.

12. Alan Turing, the notable inventor and war hero, was tasked to crack encrypted messages used by World War II's Axis Powers. *See* Robert Plotkin, *Computer Programming and the Automation of Invention: A Case for Software Patent Reform*, 7 UCLA J.L. & TECH. no. 2, 2003, at 1, 23 ("Turing helped to design and build code-breaking machines consisting of large amounts of complex and interconnected circuitry."). Historians estimate that these code-breaking machines shortened the war and saved millions of lives. *See* Jack Copeland, *Alan Turing: The Codebreaker Who Saved 'Millions of Lives*,' BBC (June 19, 2012), https://www.bbc.com/news/technology-18419691 [https://perma.cc/ZL3R-NTDL].

13. *See* Aaron Perkins, Comment, *Encryption Use: Law and Anarchy on the Digital Frontier*, 41 HOUS. L. REV. 1625, 1629 (2005) (citing *Encryption Security in a High Tech Era: Hearing Before the Subcomm. on Int'l Econ Pol'y & Trade of the H. Comm. on Int'l Rels.*, 106th Cong. 12 (1999) (Statement of Barbara McNamara, Deputy Director, National Security Agency)).

14. *See id.* at 1630 (citing Norman Andrew Crain, Comment, Bernstein, Karn *and* Junger*: Constitutional Challenges to Cryptographic Regulations*, 50 ALA. L. REV. 869, 873 (1999)). It is also worth noting that the average citizen did not use advanced computing or technologies at that point in time, and therefore did not require advanced tools to protect any data. *See* Crain, *supra*, at 873.

information and technology age, in which the average person, nearly universally, used digital information, ushering in a new age of encryption needs and solutions.[15]

Computer technologies have advanced exponentially over time, to a degree where some can make trillions of calculations per second.[16] This detail is crucial because modern-day cryptography[17] relies primarily on computing power for its strength.[18] Accordingly, the more powerful computers become, the greater the likelihood that ciphers and digital protections for sensitive data will be broken.[19] At this point, both governmental and private developers are racing to develop newer methods for encryption and decryption,[20] leading to the current status: A point where the average user can utilize potentially unbreakable encryption methods.[21]

---

15. *See* Perkins, *supra* note 13, at 1630–31 (discussing the creation of the National Security Agency (NSA) and its domination of the encryption technology space).

16. *See* Sherwinter, *supra* note 9, at 514 (citing Stephen Shankland, *IBM Set to Take Supercomputing Crown*, CNET (Nov. 5, 2004, 10:51 AM), https://www.cnet.com/tech/computing/ibm-set-to-take-supercomputing-crown/ [https://perma.cc/9MSX-SB47]). This is disregarding the emerging developments of quantum computing that will soon brandish computing power and abilities that are lightyears ahead of any technologies we currently possess. *See generally* Cason Schmit, *Intellectual Property's Upcoming Quantum Leap: Projecting the Future Challenges Facing Quantum Information Technology Through a Historical Perspective of the Computer Revolution*, 95 J. PAT. & TRADEMARK OFF. SOC'Y 271 (2013).

17. Basic encryption accessible to the average user today is practically unbreakable, and some minimally encrypted files can take years to decrypt, depending on the technology and those who attempt decryption. *See* Matthew J. Weber, Note, *Warning—Weak Password: The Courts' Indecipherable Approach to Encryption and the Fifth Amendment*, U. ILL. J.L. TECH. & POL'Y 455, 459 (2016) (citing Mohit Arora, *How Secure is AES 128 and 256 Encryption Against Brute Force Attacks?*, EE TIMES (May 7, 2012), https://www.eetimes.com/how-secure-is-aes-against-brute-force-attacks/ [https://web.archive.org/web/20220630044821/https://www.eetimes.com/how-secure-is-aes-against-brute-force-attacks/]).

18. *See* Sherwinter, *supra* note 9, at 516–19 (noting that for now, basic encryption remains viable, but the advent of quantum computing and its eventual proliferation may "render strong encryption schemes impotent").

19. *See id.* at 517.

20. *See id.* at 519. It is important to note that no one can make this assertion with complete certainty, as it is impossible to know what encryption and decryption capabilities large governments and corporations secretly possess.

21. Further popularizing the use of this software type is that it is "open source," meaning that the source code comprising the software is readily viewable and accessible to all. *See* Justin C. Colannino, *Free and Open Source Software in Municipal Procurement: The Challenges and Benefits of Cooperation*, 39 FORDHAM URB. L.J. 903, 911 (2012). This allows the public to audit software and its systems, resulting in a lower risk of bugs (errors) and fewer opportunities for security risks. *Id.*

B. Data Privacy Law in the United States

Data privacy law in the United States is developing slowly compared to other leading countries.[22] The United States' sluggishness aside, changes to privacy regulations will still not match other countries' trajectory at this rate.[23] Rather than embracing encryption and learning to adapt to its usage,[24] the United States government prevented citizens' use of encryption.[25] Ultimately, this resulted in unnecessary and prolonged litigation[26] since the government has pushed to compel technology companies to implement "backdoor access" within encryption platforms enabling the government's discretionary access.[27]

While the government's drive to access encrypted devices may appear imperative from a national security perspective, implementing "backdoor" encryption circumvention methods places an unprecedented demand upon companies that have spent years developing proprietary software. Not only would this software require drastic changes, but it would also likely play a role in creating "backdoor access" that would merely enable terrorists and other bad actors.[28] Forcibly weakening encryption will not stop people from protecting their data and will force users to find other methods to prevent unauthorized access.[29]

In 2008, Illinois codified a right to privacy in personal biometric information.[30] While other states sought to pass, or already effectively passed, new and progressive data privacy laws,[31] none have succeeded to the degree Illinois

22. *See* David B. Kahng, *The Impact of Emerging Models of Data Privacy Laws in Europe and the United States*, ACC DOCKET (Dec. 01, 2016), https://docket.acc.com/impact-emerging-models-data-privacy-laws-europe-and-united-states [https://perma.cc/8UMD-ZUY8].

23. *See id.*

24. *See infra* Section II.C.

25. *See* Lin, *supra* note 6, at 1131.

26. *See id.* at 1127–28.

27. Traylor, *supra* note 5, at 497–98 (discussing the government's attempts to compel Apple's incorporation of backdoor access to their iPhone's encryption platform).

28. *See id.*

29. *See id.* at 498 (noting that customers would just lose faith in corporations' abilities to protect their data, inferring that customers would simply look for other means of protection).

30. *See generally* Torsten M. Kracht, et al., *Recent developments under BIPA: Examining Spokeo's impact and more*, PRAC. INSIGHTS COMMENTS., 2018 WL 2381897.

31. *See id.* at 2; *see also* Al Leiva & Tracy Weir, *The New York Privacy Act: A consumer privacy bill to monitor closely*, PRAC. INSIGHTS COMMENTS., 2019 WL 3211439

has.[32] At this point, Illinois is a trailblazer in the United States and provides a private right of action for misuse of one's biometric information.[33] Although Illinois' efforts regarding personal data protections are at a more advanced stage than other states, whether data protection in the United States progresses to a point where there is comprehensive legislation for all Americans remains unclear.

C. A Comparative Perspective

While no current legal framework fully incorporates the idea of a right to encryption within their data privacy regime, some nations started to address this growing problem.[34] These jurisdictions contain some, if not the only, legal frameworks for data encryption and are addressed in turn below.

1. The European Union

Enacted in 2018, the European Union's (EU) General Data Protection Regulation (GDPR) paved the way for a robust system that embraces encryption methods and data protection rights.[35] Further, the EU established an advisory board to oversee the adoption of said system.[36] Most importantly, recent jurisprudence in the EU indicates a progressive encryption approach, favoring citizens' right to encrypt and protect their data, while still accounting for national security concerns.[37]

(discussing California's Consumer Privacy Act (CCPA) and New York's attempts to pass the New York Privacy Act (NYPA)).

32. *See* Kracht et al., *supra* note 30, at 2.

33. *Id.*

34. Nations address this problem not necessarily by enacting a right to encryption, or even an equivalent, but in some respects, by just expanding privacy and technology laws. *See* Hugh J. McCarthy, *Decoding the Encryption Debate: Why Legislating to Restrict Strong Encryption Will Not Resolve the "Going Dark" Problem*, 20 J. INTERNET L., no. 3, Sept. 2016, at 1, 25–31 (noting various responses to the encryption debate).

35. *See id.* at 32.

36. *See id.*

37. *See id.* (citing Karlin Lillington, *European Court of Justice is Human Rights Rottweiler*, IRISH TIMES (Apr. 28, 2016), https://www.irishtimes.com/business/technology/european-court-of-justice-is-human-rights-rottweiler-1.2626809 [https://perma.cc/338N-8992]). However, the GDPR's Article 23 does provide a national security exemption. Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC, art. 23, 2016 O.J. (L 119) 46–47.

2. India

India also tried to balance data encryption and national security concerns.[38] Generally, India's approach suggests a struggle with balancing security and privacy rights.[39] At various times, the Indian government proposed weakening encryption protocols to allow discretionary governmental access, subsequently withdrawing the proposal just days later.[40] India has yet to implement a more permanent policy or suggest another proposal in the meantime.

III. WHY DO WE NEED ENCRYPTION?

In addition to an innate predisposition to keep one's communications private, society has morphed into an information-based culture where most are conscientious of safeguarding their data.[41] However, using electronic systems without proper safeguards is akin to "relying solely on postcards in the mail, replacing envelopes with blind trust."[42] This is where encryption comes into play. Encryption methods offer a layer of protection for digital assets that prevent third-party intrusions, protecting data from any unauthorized access.[43] While society must consider governmental interests, citizens' private data has long been abused and infringed upon in a way that citizens can only thwart with widespread access to encryption.[44]

In addition, government data breaches are occurring at an astounding and worrisome rate.[45] The government holds colossal amounts of its citizens'

38. *Id.* at 30 (discussing the Indian government's concerns in the aftermath of the 2008 Mumbai bombings).

39. *See id.*

40. *See id.* (citing John Ribeiro, *India Withdraws Draft Encryption Policy Following Controversy*, PCWORLD (Sept. 22, 2015, 2:34 AM), https://www.pcworld.com/article/423651/india-withdraws-draft-encryption-policy-following-controversy.html [https://perma.cc/2P97-J75S]).

41. *See* Timothy B. Lennon, Comment, *The Fourth Amendment's Prohibitions on Encryption Limitation: Will 1995 Be Like 1984?*, 58 ALB. L. REV. 467, 471 (1994).

42. *Id.*

43. *See id.* at 472 (pointing out that encryption defends against unauthorized access by government as well as third parties).

44. *Id.* at 475.

45. *See* A. Michael Froomkin, *Government Data Breaches*, 24 BERKELEY TECH. L.J. 1019, 1027 (2009).

private data,[46] and its protection is woefully inadequate.[47] Worsening matters, data legally obtained by the government is often subject to illegal disclosure.[48] While the government must protect private data from exploitation, the government rarely conducts itself within the confines of the privacy and data breach laws it has established for others.[49] Understandably, these privacy violations solidify citizens' mistrust of the government regarding their data protection rights.

Finally, the United States' current legal landscape regulates reactively and is, therefore, unsuited to cope with the swiftly-developing technology world.[50] American privacy law lacks a conclusive structure and its ambiguity significantly affects the public-choice landscape regarding privacy and data encryption.[51] The only way to protect people in the new era of data proliferation is to establish a regime that recognizes one's right to encrypt personal data and protect it the same way one would protect tangible property. In contemplating the need for balance between governmental and personal interests, this solution will also require exceptions to the proposed right coupled with a strategy for transparent oversight.[52]

A. The Technology: Relevant Encryption Methods

Today, most of the average person's technology-based activities include some type of encryption.[53] Scholar Riana Pfefferkorn, who researches the impacts of cybersecurity and electronic surveillance on Fourth Amendment privacy, aptly stated:

> Encryption started out being too important to let just anybody use it. But in the digital age, it has become too important for anybody *not* to use it. We rely on

46. *Id.* at 1022.
47. *See id.* at 1027.
48. *See id.* at 1051 (citing Doe v. Chao, 540 U.S. 614, 616–17 (2004)).
49. *Id.* at 1058–59 (discussing government's propensity to exempt themselves from data breach laws).
50. Lior Jacob Strahilevitz, *Toward a Positive Theory of Privacy Law*, 126 HARV. L. REV. 2010, 2035–36 (2013).
51. *See id.* at 1035–37.
52. Including recourse for government entities that must access data in certain pressing scenarios.
53. *See* Paul McLaughlin, Comment, *Crypto Wars 2.0: Why Listening to Apple on Encryption Will Make America More Secure*, 30 TEMP. INT'L & COMPAR. L.J. 353, 355 (2016) (citing Charles Arthur, *How Internet Encryption Works*, GUARDIAN (Sept. 5, 2013, 3:19 PM), https://www.theguardian.com/technology/2013/sep/05/how-internet-encryption-works [https://perma.cc/JD3W-LAD9]).

> encryption to secure our communications, medical records, banking records, financial transactions, business secrets, intellectual property, and national security.[54]

Technology companies have incorporated encryption software into most programs and systems employed by the end-user to bolster their users' privacy and safety.[55] These companies believe that complete encryption is crucial to protect user data and are strong proponents of users' ability to exercise encryption.[56] This remains especially true today, in an age where personal computing is an integral aspect of daily life.[57]

The average person in the United States now uses technological devices to store potentially sensitive photos, music, documents, and videos, among many other types of digital information.[58] Encryption is more than necessary to protect and prevent unauthorized access to personal data,[59] the same way one stores documents in a safe or locks their front door at nighttime.

1. Basic Concepts of Data Encryption

Though the technical minutia of encryption is essential to its functionality, the basis of this Article's proposition requires only a rudimentary understanding of encryption.[60] Although one can explain the concept of encryption in readily understood terms, its varied concepts range from simple terms and

54. Pfefferkorn, *supra* note 7, at 1402 (footnotes omitted) (first citing Ann Cavoukian, *Encryption is Crucial to Our Privacy and Freedom*, GLOBE & MAIL (Dec. 9, 2015), https://www.theglobeandmail.com/opinion/encryption-is-crucial-to-our-privacy-and-freedom/article27652852/ [https://perma.cc/W626-5YF4]; and then citing Susan Landau, The National-Security Needs for Ubiquitous Encryption, *in* DON'T PANIC: MAKING PROGRESS ON THE "GOING DARK" DEBATE app. A 1–3 (Berkman Ctr. for Internet & Soc'y at Harv. Univ. 2016)).

55. Technology companies have also incorporated encryption software for other, less altruistic, purposes including "to bolster their bottom line." *See* McLaughlin, *supra* note 53, at 355.

56. *See id.* at 360–61 (arguing that providing government or law enforcement with special access is not feasible). For an example of the detrimental impact of data breaches on individuals, see Rob McLean, *A Hacker Gained Access to 100 Million Capital One Credit Card Applications and Accounts*, CNN BUS. (July 30, 2019, 5:17 PM), https://www.cnn.com/2019/07/29/business/capital-one-data-breach [https://perma.cc/FFP3-XSPT].

57. *See* Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, 8 J. TELECOMM. & HIGH TECH. L. 359, 363 (2010).

58. *See id.*

59. *See id.* at 372–79.

60. A more technical discussion regarding encryption computing is beyond the scope of this Article.

features to complicated mathematical and technical details.[61] This Article addresses the notion of "encryption" concerning its technical context within the realm of data encryption. Hence, encryption refers to a process, or tool that enables such a process, that obfuscates or otherwise cloaks data so only those permitted can access said data.[62] Generally, computer programs use some form of cryptography[63] to create a key that encrypts data to render it ostensibly unreadable.[64] After which, that key—or another key, if so chosen—can decrypt the data, once again enabling access.[65]

Many commonly used encryption programs and systems rely on established algorithms that securely encode data.[66] As technology developed, encryption methods grew more prolific; many modern devices used daily possess sophisticated encryption capabilities.[67] At present, most cell phones have encryption capabilities that prevent unauthorized parties from accessing data.[68] Not only is this convenient for the average user, but it is necessary due to potentially sensitive information stored within one's phone.[69]

2. Readily Available Tools

This section will examine some of the encryption methods available to and presently used by the average end-user.[70] The purpose is to illustrate

---

61. *See* Perkins, *supra* note 13, at 1627–29 (discussing the basic terms, concepts, and terminologies of encryption).

62. *See id.* (citing Crain, *supra* note 14, at 871).

63. "Cryptography" refers to the art of writing or solving codes, generally to encrypt information. *See id.* at 1627–28.

64. *See id.* at 1628 (citing Crain, *supra* note 14, at 871).

65. *See id.*

66. *See id.* (discussing the use of publicly available algorithms and noting that algorithms that rely on secret or hidden source code are of suspect integrity and nature).

67. *See id.* at 1627. Further, the emergence of global internet also enabled users to gain access to increasingly advanced encryption methods. *Id.* at 1657.

68. *See* Jack Pringle, *From Breaking Down Doors to Building Back Doors: The FBI-Apple Case is Only the Latest Battle Pitting Privacy Against the Need to Investigate Crime*, S.C. LAW., Jan. 2017, at 34, 35 ("[The] iPhone . . . offers users the ability to 'lock' the device . . . with a passcode."). Many devices come standard with encryption, and hundreds of millions of users have access to messaging and email apps with built-in encryption, such as Telegram, WhatsApp, and Gmail. *See* McLaughlin, *supra* note 53, at 356–58.

69. *See* Riley v. California, 573 U.S. 373, 403 (2014) (discussing the secrets and "privacies of life" contained on any given individual's phone, how that information is worthy of the utmost protection, and how it is reasonable to expect this privacy to extend to all of one's electronic devices (quoting Boyd v. United States, 116 U.S. 616, 630 (1886))).

70. These methods are outlined below. Notably, they do not require any technical training or extensive knowledge for their use. Any competent computer or technology user can make use of these programs by following their respective instructions and deployment guides.

that the average technology user can now use free tools to protect their data, not only from hackers and those seeking to perpetuate harm, but also from the government.[71]

To start, perhaps the most profound among these accessible encryption tools is end-to-end encryption.[72] End-to-end encryption is a coding method involving two keys—one public and another private.[73] Due to the incredibly high degree of privacy afforded by this data encryption method, it is used across the technology space and embedded in various systems used daily by countless individuals.[74] This encryption method enshrouds information from service providers or application administrators who control the medium.[75]

a. Pretty Good Privacy

Developed by Phil Zimmerman in 1991, Pretty Good Privacy (PGP) was one of the first programs of its kind: One that allowed the average user, with basic hardware, to encrypt and digitally secure their messages and transmissible data.[76] Before the advent of PGP, it was comically easy for the government to control encryption.[77] Because encryption tools and hardware were costly, the average user did not have sufficient resources to protect their data adequately.[78] However, PGP enabled individuals to

71. The government has relied on preexisting interpretations of federal law to compel private companies to hand over individuals' private Secure Socket Layer (SSL) encryption keys. *See* Pfefferkorn, *supra* note 7, at 1418 (citing United States v. Lavabit, LLC., 749 F.3d 276, 287–89 (4th Cir. 2014)).

72. The propagation of which has spread data encryption to users throughout the globe. *See* McLaughlin, *supra* note 53, at 357.

73. Keys are devices or algorithms that are used to encode information. *See id.* at 355 (citing *Encryption Technology and Possible US Policy Responses: Hearing Before the Subcomm. on Info. Tech. of the Comm. on Oversight & Gov't Reform*, 114th Cong. 58 (2015) (statement of Matthew Blaze)).

74. *See id.* at 355–57.

75. Facebook, who owns WhatsApp, a popular messaging application, cannot observe, gather, or access its users' messaging data because of this encryption. *See id.* at 357–58.

76. *See* Lennon, *supra* note 41, at 476 (citing Ronald Bailey, *Code Blues*, REASON, May 1994, at 36, 37).

77. *See id.*

78. *See id.* ("The advent of effective, low-cost methods of computerized encryption was one factor leading to a heightened level of governmental concern over private secrecy.").

protect their private information against unauthorized access.[79] At this time, the government began to worry about its ability to access citizens' private data for legitimate purposes.[80]

b. BitLocker

Data stored on one's computer or removable storage devices are susceptible to unauthorized access.[81] BitLocker is an encryption suite that allows Windows Operating System (OS) users to encrypt their removable and non-removable data storage devices.[82] The average OS user is not aware that third parties may easily bypass an OS password security feature—for example, a Windows or Mac user profile—simply by removing the data drive or accessing the drive without booting up the OS.[83] BitLocker provides strong encryption that prevents all unauthorized access to encrypted drives;[84] while this prevents government investigators from seizing files on such devices, BitLocker keeps users' data secure.[85] Notably, this encryption tool only encrypts entire data drives and does not provide single-file encryption.[86]

---

79. *See* Woodrow Hartzog, *The Fight to Frame Privacy*, 111 MICH. L. REV. 1021, 1036 (2013) (citation omitted).

80. *See id.* at 1037 (discussing the government's argument for access to encryption keys in the name of national security).

81. *See* DEREK MELBER, WINDOWS AUDIT UPDATE: WINDOWS 7 SECURITY FEATURES: BITLOCKER AND BITLOCKER TO GO (Warren Gorham & Lamont 2009), 2009 WL 7296916.

82. *See id.*

83. Even if one uses the most secure passcode for their OS user account, it may be circumvented easily if the drive itself is not encrypted. An OS's security is only active if the user boots up into the system itself. When an unencrypted drive is accessed without booting into the OS, another computer or separate OS can read the information as if it was simply another drive inserted into the computer. *See How to Access Microsoft Windows Files and Folders from Linux*, LINUXBSDOS (Jan. 2, 2012), https://linuxbsdos.com/2012/01/02/how-to-access-microsoft-windows-files-and-folders-from-linux/ [https://perma.cc/2YNR-GVV7].

84. For more information about Microsoft's BitLocker documentation, see BITLOCKER, https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview [https://perma.cc/2B9R-WYM3].

85. *See* Wachtel, *supra* note 9, at 51 (noting that Bitlocker is a "[s]trong encryption program[]"); *see also* Aloni Cohen & Sunoo Park, *Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries*, 32 HARV. J.L. & TECH. 169, 177 (2018) (explaining that an encryption is only as good as the password facilitating it, and that each additional character in a password exponentially enhances its complexity).

86. For a free, single-file encryption tool, see *infra* Section III.A.2.c.

c. VeraCrypt

Unlike BitLocker, VeraCrypt[87] is a free encryption suite that can protect individual files, entire operating systems, and complete storage drives.[88] Aside from its versatility and vast selection of different encryption methods, VeraCrypt also provides users with a plausible deniability feature powerful enough to hide the existence of protected information altogether.[89] Overall, this is an exceptional tool for protecting one's data, and it has even prevented expert forensic examiners from accessing data drives in the past.[90]

d. Cloud Encryption

Many people use cloud encryption, and often without personal knowledge of their doing so. At this point, most major companies' websites and online service providers use HTTPS encryption protocol to protect data transmitted over the internet.[91] Cloud encryption protects internet users from hackers and third parties seeking to capture users' data and ensures that only the intended recipients can read it.[92] Within most contexts online, users need not configure settings manually; they can simply use the intended website and remain secure in knowing their data is protected.[93] While not all platforms use HTTPS as their default protocol, it is quickly becoming an industry standard.[94]

---

87. VeraCrypt is available for download. VERACRYPT, https://www.veracrypt.fr/en/Downloads.html [https://perma.cc/NJS2-8NN7].

88. *See* Cohen & Park, *supra* note 85, at 203.

89. *Id.* at 203; *see also id.* at 203–04 ("[T]o compel the production of files hidden by deniable encryption, the government would need to establish knowledge of the 'existence of the hidden files' along with 'the location of the requested files with reasonable particularity.'" (quoting Timothy A. Wiseman, Encryption, *Forced Decryption, and the Constitution*, 11 I/S: J.L. & POL'Y 525, 573 (2015))).

90. *See id.* at 201.

91. HTTPS stands for Hypertext Transfer Protocol Secure. Soghoian, *supra* note 57, at 375; *see also id*. at 375–76 (detailing how HTTPS protects data traveling to and from websites).

92. *See id.* at 375.

93. *Id.* at 376.

94. *See id.* at 378 (discussing Google's decision to adopt encryption by default within Gmail, and Facebook, Microsoft, and Yahoo's reluctance to do so); *see also Why HTTPS for Everything?*, CIO, https://https.cio.gov/everything/ [https://perma.cc/7GVD-7M46] ("HTTP is currently the primary protocol for applications used on computers, tablets, smartphones, and many other devices.").

e. Signal

As one of many free messaging apps, Signal[95] uses end-to-end encryption to protect messages, voice calls, and video calls.[96] Users need not possess knowledge of encryption or technical skills to use the application; one can simply install it and begin to send encrypted messages.[97] Other messaging apps, like Facebook's WhatsApp, Apple's iMessage, and Telegram use end-to-end encryption—or even Signal's encryption protocol—to protect their users' communications.[98]

f. Blockchain Encryption

Although blockchain encryption is not as readily accessible to the average technology user, its increasing prevalence in the technology space warrants mention. Blockchain encryption works by indelibly storing transactions on a public "ledger."[99] Users may employ this encryption method to ensure that documents and files are not tampered with by utilizing blockchain encryption's logging feature, which individuals cannot alter without detection.[100]

g. Biometric Security

In one of its most prolific usages, millions of people protect their devices with biometric security and encryption.[101] Manufacturers continue to

95. Signal is available for download. SIGNAL, https://signal.org/en/download/ [https://perma.cc/2FHR-R9JZ].

96. Pfefferkorn, *supra* note 7, at 1404 (first citing Cade Metz, *Forget Apple vs. the FBI: WhatsApp Just Switched on Encryption for a Billion People*, WIRED (Apr. 5, 2016, 11:00 AM), https://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/ [https://perma.cc/TY7D-LMDQ]; and then citing Martin Shelton, *Upgrading WhatsApp Security*, MEDIUM (Feb. 6, 2017), https://medium.com/@mshelton/upgrading-whatsapp-security-386c8ce496d3 [https://web.archive.org/web/20170210184944/https://medium.com/@mshelton/upgrading-whatsapp-security-386c8ce496d3]).

97. *See id.*

98. *See id.*

99. Michael Cross, *Rocket Lawyer Offers 'Smarter Transactions' with Bitcoin Technology*, LAW SOC'Y GAZETTE (Sept. 6, 2018), https://www.lawgazette.co.uk/practice/rocket-lawyer-offers-smarter-transactions-with-bitcoin-technology/5067436.article [https://perma.cc/PZ5E-N2YP] ("Blockchain, best known for enabling virtual currencies such as Bitcoin, works by creating a constantly updated record of transactions across a so-called shared ledger.").

100. *See* Charles Cresson Wood, William S. Rogers Jr., & Ralph Spencer Poore, *Why It's Now Time for an Internationally Harmonized Legal Regime for Information Security and Privacy*, 14 ABA SCITECH LAW., no. 3, Spring 2018, at 20, 22.

101. *See By 2024, How Many Smartphone Owners Will Use Biometrics?*, PAYMENTS JOURNAL (June 4, 2020), https://www.paymentsjournal.com/by-2024-how-many-smartphone-

implement biometric security features that allow users to unlock their phones without passwords.[102] However, this method of securing one's device is markedly different from the preceding encryption methods. In an unfortunate trajectory, United States courts failed to accord biometric security platforms with the same rights afforded to a traditional password.[103] Instead, many courts allow law enforcement to compel users to unlock their devices encrypted with biometric security, practically rendering it useless—at least in some regards.[104] Considering the courts' varied approaches to technology and encryption, users should familiarize themselves with their jurisdiction's treatment of security, encryption, and privacy rights.[105]

As stated, the methods above are a small sampling from a multitude of available encryption tools and platforms. Current technology users have many safe, reliable, and free encryption tools at their disposal; most are merely a few clicks away.

IV. LEGAL DISCUSSION: THE CONFLICT

Part IV discusses current conflicts that permeate the data privacy and encryption discourse in society. Namely, the idea that people can protect their personal data to a degree that even the government cannot readily access and government interests in accessing that data for presumably lawful reasons.

A. Government's Interests and Privacy Rights

The United States underwent a drastic change in the last few decades, not only within the technology industry but also in how the country strikes

owners-will-use-biometrics/ [https://perma.cc/5EDW-9GLT] (discussing current estimations for smartphone users who utilize biometric security).

102. Weber, *supra* note 17, at 471 (citing Mehedi Hassan, *How Biometrics on Smartphones is Changing Our Lives*, M2SYS: BLOG (July 13, 2016), https://www.m2sys.com/blog/biometric-resources/biometrics-on-smartphones/ [https://perma.cc/5RWT-UA3K]).

103. *See id.* (first citing United States v. Hubbell, 530 U.S. 27, 35–36 (2000); then citing Fisher v. United States, 425 U.S. 391 (1976); and then citing Commonwealth v. Baust, 89 Va. Cir. 267, 271 (2014)).

104. *See id.* at 471–72 (discussing *Baust*, *Hubbell*, and *Fisher*).

105. *See id.* at 472 ("As it is such a new technology, it is still unclear if other courts will interpret fingerprints or other biometrics as testimonial; or follow the lead of the Virginia court and liken it to providing other non-testimonial evidence.").

a balance between personal liberties and national security.[106] What began as reactionary maneuvers to Cold War threats quickly evolved into the government's drive to develop and advance its intelligence capabilities, striving to combat perceived threats of international terrorism.[107] Complicating matters, the nation's enemies understand that the law of the land prevents the government from gaining tactical and strategic advantages, as the government constrains its actions to remain within the country's legal framework.[108] Eventually, this precipitated governmental attempts to legally access its citizens' private data and information for the sake of national security.[109] Perforce, the government faces a daunting challenge: Balancing society's national security needs together with its citizens' rights to liberty and privacy.

Further, the United States lacks sufficient legal protections for citizens' data.[110] The legal system has yet to recognize that the expectation of privacy extends to electronically stored data.[111] This predicament underlies an imbalance in competing interests, particularly between the government's objectives—securing national and local security and prosecuting criminals—and the average citizens' desire to maintain their privacy and well-being. Because the average technology user can readily access robust encryption tools, law enforcement and government agencies face a novel and arduous task attempting to access their data.[112]

Finally, the emergence of affordable encryption platforms greatly diminished —if not vanquished—the government's ability to access personal encrypted data with or without a warrant.[113] In the wake of revelations detailing the United States government's practices of data "snooping" and collection, citizens are now less likely to accept the government's ability to access their data.[114] Society is starkly different from the days of the early 2000s. Citizens are increasingly worried about "Big Government" intrusions into their privacy and data, with less attention and support for the government's

---

106. *See generally* Geoffrey S. Corn, *Encryption, Asymmetric Warfare, and the Need for Lawful Access*, 26 WM. & MARY BILL RTS. J. 337 (2017) (discussing the United States' reactionary responses to the Cold War and the constant need for further developments in the intelligence community simply to stay ahead of potentially adversarial countries).

107. *See id.* at 338 (noting that the government's national security objectives are now focused on combatting transnational terrorist organizations).

108. *See id.* at 339.

109. *See id.* at 342–43 (discussing government's attempts to have technology manufacturers build "backdoor access" into their devices so that the government may access encrypted data should the need arise).

110. *See* Lin, *supra* note 6, at 1094.

111. *See id.*

112. *See id.* at 1096.

113. *See id.* (citing *Security Now!: Shocked by the Shell*, TWIT (Oct. 1, 2014), https://twit.tv/shows/security-now/episodes/475?autostart=false [https://perma.cc/9PJN-WWVT]).

114. *See id.*

ability to access private information to satisfy its objectives.[115] Understandably, there is a need for clarification and a specific legal framework to address this issue. This framework must balance the government's interest in lawful access to private data with an individual's ability to protect their data from unlawful access, which is inherent in the very right this Article proposes.

B. Fourth Amendment Ambiguities

The Fourth Amendment offers strong privacy protections for our physical spaces, such as the home.[116] It also provides strong protections for private communications and requires warrants supported by probable cause before the government can eavesdrop on one's private communications, no matter how easily it can do so.[117] However, a quandary remains: Does the Fourth Amendment protect personal data, and if so, to what extent?

Courts have grappled with this question to a degree.[118] While the courts held that one could maintain a reasonable expectation of privacy—a standard on which Fourth Amendment protections hinge—in information voluntarily shared with a third party, the courts did not extend protections to stored communications, such as email.[119] This might help combat those who contend that privacy is forfeited once data is disseminated to others but does almost nothing to solve the matter.[120] Without a legal framework

115. *See id.* (explaining that "interest in strong encryption has increased" since the Snowden revelations).

116. *Id.* at 1098 (quoting Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1209 (2004)); *see also* Shlomit Yanisky-Ravid & Kyle Fleming, *Facial Recognition: Tripartite Model: Bridging the Gap Between Privacy, Public Safety, Technology and the Fourth and First Amendments* (2022) (unpublished manuscript) (on file with NOTRE DAME JOURNAL OF LAW, ETHICS & PUBLIC POLICY).

117. *See id.* at 1100 (discussing United States v. Smith, 978 F.2d 171 (5th Cir. 1992), and whether warrantless tapping of cordless phones is permissible).

118. *See id.* at 1101–03 (listing court decisions and discussions regarding potential Fourth Amendment protections for data-related communications); *see also* Yanisky-Ravid & Fleming, *supra* note 116.

119. *See id.* at 1102–03 ("Many types of storage and communication are protected by the Fourth Amendment. However, stored communication, such as e-mail, is not protected by the Fourth Amendment.").

120. Fourth Amendment protections are insufficient to (1) protect the individual's privacy rights in basic stored data, and (2) bring us any closer to a solution regarding any consideration between government's need to access private data and infringement on personal privacy.

clarifying a fundamental right to data protection, "uncertainties regarding Fourth Amendment protection[s] . . . will likely lead to mass adoption of strong encryption."[121]

C. The Fifth Amendment's Failure to Ameliorate

The government's hunt for private data is a chief factor contributing to the public's embrace of data encryption. Recently, authorities have compelled private parties to permit government access to encrypted data under the antiquated All Writs Act of 1789 (AWA).[122] Some attempt to defend against such governmental actions by asserting Fifth Amendment protections,[123] but they are not always successful.[124] While the relevant case law remains unsettled, the government's attempts to compel encryption key disclosures can trigger Fifth Amendment protections.[125] However, this is not something on which one should rely.[126]

The Fifth Amendment is not particularly suited to defend private information from the outset.[127] Instead, the Fourth Amendment is more apt for privacy concerns.[128] Moreover, this is partly due to the Fifth Amendment's protections turning on a distinction between testimonial and nontestimonial acts.[129] The Fifth Amendment's protections, based on case law, specify a requirement for a "testimonial" nature to trigger the right against self-incrimination.[130] In the end, there is strong contention that the court should not treat utilizing

---

121. *See* Lin, *supra* note 6, at 1127 ("Mass adoption of strong encryption will lead to dire security, social and economic implications.").

122. Traylor, *supra* note 5, at 490 (citing 28 U.S.C. § 1651).

123. *Id.* (explaining that parties compelled under this act have objected on two grounds: (1) the AWA does not grant the government the power to compel decryption and (2) compelling them to do so is unconstitutional); *see also* U.S. CONST. amend. V ("No person . . . shall be compelled in any criminal case to be a witness against himself.").

124. Lin, *supra* note 6, at 1112 (arguing that the government's compelling encryption key disclosure may be a violation of the right against self-incrimination and is not always successful because "[c]ourts are currently divided on" this defense).

125. *See id.* at 1128 ("[T]he Eleventh Circuit held that 'decryption and protection of the contents of the hard drives would sufficiently implicate the Fifth Amendment privilege.'" (quoting *In re* Grand Jury Subpoena Duces Tecum dated March 25, 2011, 670 F.3d 1335, 1346 (11th Cir. 2012))).

126. *See id.* (noting that the issue with strong encryption may not be solved by court orders because decryption is not feasible).

127. *See* Fisher v. United States, 425 U.S. 391, 401 (1976).

128. *See id.*

129. *See* David W. Opderbeck, *The Skeleton in the Hard Drive: Encryption and the Fifth Amendment*, 70 FLA. L. REV. 883, 901–02 (2018).

130. *See id.*

encryption software as "testimonial 'speech,'" and thus worthy of Fifth Amendment protections.[131]

Considering the dearth of any practical and conclusive avenues for recourse, it is imperative to establish an alternative legal framework. There is a need for a system by which the government can compel or gain access to private data without utterly eviscerating the individual's rights and sense of privacy.

D. Other Proposed Resolutions in The Field

As technological data in the United States becomes more prevalent, the need to balance data protection concerns against governmental interests intensifies. While many propose solutions to this predicament, one thing remains clear: Congress is the correct government entity to address this adequately, and courts have proven less than helpful in ameliorating the polarity between data encryption and governmental access.[132] This Article proposes several alternative solutions for data protection and aims to balance the proposed right of data encryption and other means of protecting an individual's private data. Many agree that governmental attempts to control encryption are futile.[133] However, this Article addresses, examines, and eventually rejects several alternative solutions.

1. Backdoor Access

As discussed above, the government and its proponents have repeatedly pushed to compel companies to implement "backdoor access" within their encryption platforms.[134] However, doing so would not prevent users from adopting robust encryption methods.[135] As a result, any attempts would

131. *Id.* at 916 (arguing that not only is encryption software use unprotectable under the Fifth Amendment, but compelling users to reveal passwords or produce encryption keys would not violate the Fifth Amendment unless the password or key itself would serve to incriminate the user).

132. *See* Traylor, *supra* note 5, at 512.

133. *See* Staci I. Levin, Note, *Who Are We Protecting? A Critical Evaluation of United States Encryption Technology Export Controls*, 30 LAW & POL'Y INT'L BUS. 529, 550 (1999) (citation omitted).

134. *See supra* Section II.B.

135. *See* Lin, *supra* note 6, at 1132 (citing *Security Now!: Your Questions, Steve's Answers 217*, TWIT (Aug. 25, 2015), https://twit.tv/shows/security-now/episodes/522 [https://perma.cc/N2NZ-U8DC]).

only cause other complications—economic, social, or otherwise.[136] Rather, the United States should implement legal protections that "conform with modern privacy expectations."[137]

2. Key Escrow

Under the Key Escrow approach, whenever a user activates encryption software, aside from generating a private "key" or method to decrypt the information, the system produces a separate key held in escrow by a trusted third-party.[138] Then, pursuant to a court order, that third-party divulges the access key to the proper authorities as needed.[139]

While this may sound like a feasible and ideal solution, the technical aspects of evolving encryption render it unimplementable.[140] First, an encryption system frequently changes the keys with which it encrypts data and updating that key with a third party in each instance could be unduly cumbersome.[141] Second, users would need to trust whatever third-party is involved.[142] This would be akin to the government mandating that citizens store a copy of their house keys with a third party, just in case law enforcement deem it necessary to enter their homes. Considering that encryption already revolves around a fundamental distrust of others, many would be hard-pressed to find a fiduciary suitable to store encryption keys securely.

3. Outright Bans, the Fourth and Fifth Amendments, & Weak Encryption

As discussed, the Fourth and Fifth Amendments to the United States Constitution provide little-to-no help in resolving the data encryption issue. Additionally, attempts to ban or weaken encryption standards are entirely impracticable options.[143] Simply perusing pertinent literature on this matter clarifies the need for a fundamental change in the United States' data protection system.

---

136. *See id.* at 1131–33 (noting that the economy and other aspects of society will suffer if the government intervened to hamper its citizens' encryption use).
137. *Id.* at 1135.
138. McCarthy, *supra* note 34, at 29.
139. *Id.*
140. *See id.*
141. *See id.* (citing THE INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2015 apps. A1, at 67 (Europol 2015)) (requiring this would be akin to having someone alert a third-party each time they accessed their private data—by encrypting and decrypting it—and that could happen many times on any given day).
142. *See id.*
143. *See id.* at 29–31.

V. THE RIGHT TO DATA ENCRYPTION

A. The Benefits of Implementing Formal Protection

In the absence of a suitable legal framework to address data privacy and individuals' right to data protection, this Article recommends that the legislature create and recognize an innovative right: The Right to Data Encryption. This is a narrow proposal by design; it posits a negative and not a positive right. Therefore, it would not be the government's burden to provide anyone with the means to encrypt their data. Rather, this right would exist to protect those who encrypt their data by any means they choose. Instead of spawning yet another new governing agency to monitor data privacy and protection,[144] legislators should implement the right to data encryption without creating entirely new government entities.

Next, this Article posits a novel concept: That digital property is equivalent to tangible property.[145] Therefore, individuals should have the same expectation of privacy and control for their digital information. Further, the government should provide the same rights for citizens, as are afforded to tangible property, to defend their digital property from others.[146] The right to encrypt one's data begets the need and desire to protect private digital assets.[147] This right would allow technology users to employ whatever means necessary to protect their data,[148] eventually culminating in a regime that respects an individual's right to utilize any available encryption methods and safeguard their precious information from third-party intermeddlers.[149] Subsequently, Part V discusses various perspectives justifying this right.

---

144. *See* McCarthy, *supra* note 34, at 31.

145. *See generally* I. Trotter Hardy, *Not So Different: Tangible, Intangible, Digital, and Analog Works and Their Comparison for Copyright Purposes*, 26 U. DAYTON L. REV. 211 (2001) (arguing that in the context of copyright laws, it does not matter whether the work is digital or non-digital). This is certainly a controversial idea, but a developing one nonetheless.

146. *See id.* at 217 (proposing the idea that individuals should use encryption platforms to protect their digital works if there are methods—and this Article describes several—available to them).

147. Some have even argued that the government should leave the issue of data protection entirely and instead allow for the individual to utilize encryption in a form of "self-help" to protect their data. *See id.* at 212–13.

148. The same way one can purchase whatever sort of vault, lock, or security system for their property.

149. Be it hackers, terrorists, thieves, or even the United States Government.

1. Opposition to Data Encryption Rights

However, were one to reject this approach, there would still be a modicum of recourse for data protection rights in the United States.[150] The United States sorely lacks definitive laws that afford fundamental data protection rights.[151] Instead, any existing laws that support technology users exist solely on an industry-by-industry basis and often vary on state and federal levels.[152] Some propose a "judicially enacted writ of habeas data,"[153] similar to that of certain Latin American countries that provide citizens with extensive data rights.[154] However, like the right to data encryption, this is a mere proposal and has yet to see implementation in the United States.[155] Therefore, to rely on options other than congressional action is a slippery slope because such avenues may not produce any formal, legal protections substantially more significant than full-fledged data encryption rights.

B. Balancing the Proposed Right to Data Encryption

Like other rights afforded to citizens in the United States, the proposed legislation should contain exceptions for governmental interests.[156] While conclusive propositions would require extensive research, data-based investigations, and surveys of potential social ramifications—elements that are beyond the purview of this Article—potential exclusions within this right could help balance individual liberties with governmental interests.

First, the right to data encryption can include a modified warrant system like that of the criminal justice system,[157] pursuant to which a designated court can determine whether there is probable cause and reasonable

150. *See generally* Sarah L. Lode, Note, *"You Have the Data" . . . the Writ of Habeas Data and Other Data Protection Rights: Is the United States Falling Behind?*, 94 IND. L.J. (SUPP.) 41, 56 (2019) (discussing the United States' approach to data protection and its "patchwork quilt" composition).

151. *See id.*

152. *See id.* (citing Lisa J. Sotto & Aaron P. Simpson, *United States*, *in* GETTING THE DEAL THROUGH: DATA SECURITY & PRIVACY 208, 208 (Rosemary P. Jay & Hutton & Williams eds, Law Business Research 2015)).

153. *Id.* at 63.

154. *Id.* at 43 (citing Marc-Tizoc Gonzalez, *Habeas Data: Comparative Constitutional Interventions from Latin America Against Neoliberal States of Insecurity and Surveillance*, 90 CHI.-KENT L. REV. 641, 642 (2015)).

155. *See id.* at 63.

156. *See* Richard H. Fallon, Jr., *Strict Judicial Scrutiny*, 54 UCLA L. REV. 1267, 1332–33 (2007) (discussing efforts to identify government's compelling interests and when they may supersede individual rights).

157. *See* United States v. Peralta, 361 F. Supp. 3d 313, 320 (N.D.N.Y. 2019) (discussing the court's task of making "practical [and] common sense" decisions whether circumstances allow for a warrant pursuant to the Fourth Amendment (quoting United States v. Serrano, 937 F. Supp. 2d 366, 372 (E.D.N.Y. 2013))).

circumstances necessitating governmental access to encrypted data.[158] Next, if government authorities seek access to encrypted data and the relevant parties defy court ordered compulsion, the legislated right can include monetary or other penalties to encourage compliance. This would contain many similarities to scenarios in which law enforcement demands that one unlocks their home or allows access to their property, or in which law enforcement otherwise gains entry through brute force.[159] However, because governmental agencies cannot "kick in" encryption as they would a door, the right's exceptions must contain alternate options to compel compliance, such as the aforementioned warrant process or other means of judicial enforcement.[160]

Finally, the right should include a comprehensive appeal process allowing subjects of governmental access the opportunity to appeal decisions made by preceding judicial or grand jury decision processes. While this may considerably retard the process, it is simply the collateral cost of preventing the government from trampling privacy and personal data encryption rights.

As with any federally-proposed legal protection, there are certainly earmarking opportunities and bargaining chips that legislators will use upon its evaluation and any ensuing deliberations.[161] Suggesting the warrant system and appeals process in the first round of such political discussions may help contextualize some sacrifices to either bureaucratic efficiency or the absolute protection afforded by this right. To ensure its place in law as a new formal right, Congress must consider these exceptions during the legislative process.

---

158. *See generally* Susan M. Schiappa, Note, *Preserving the Autonomy and Function of the Grand Jury:* United States v. Williams, 43 CATH. U. L. REV. 311 (1993) (discussing the grand jury's purpose of protecting innocent people from unjust government prosecution).

159. *See, e.g.*, Marshall v. Barlow's, Inc., 436 U.S. 307 (1978) (warrantless search of business property).

160. Perhaps requiring any "warrant" approvals to not only require a judge's approval, but the approval of quasi-grand jury. That way, there are further limits on how easily government can gain approval for access to protected data. For further discussion of how the government can access property through warrants and subpoenas, see Jonathan F. Bloom, Note, *Entries and Searches in the Administrative Setting*, 53 GEO. WASH. L. REV. 230, 235 (1985).

161. *See generally* Norman Ornstein, *Pork Barrel Spending Returns, More Transparent and Hopefully Without the Corruption*, USA TODAY (Mar. 3, 2021, 3:15 AM), https://www.usatoday.com/story/opinion/2021/03/03/pork-spending-local-projects-requirements-prevent-abuse-column/6876840002/ [https://perma.cc/N8AM-P322].

VI. THEORETICAL JUSTIFICATIONS FOR THE RIGHT TO DATA ENCRYPTION

Several theoretical justifications for the right to data encryption support congressional legislation as the most logical means moving forward. This Part addresses the right to data encryption relating to John Locke's Labor Theory, the theory of Personality and Autonomy, alternative legal frameworks, and potential Law and Economics justifications.

A. Data Encryption & Locke's Labor Theory

Locke's theory posits that God bequeathed the world to humankind and that man would share its contents in common.[162] However, Locke postulated that once an individual mixed his labor with common resources, it became his property.[163] Locke held that one maintained ownership, not just in intangible property but in personhood and rights; necessarily, it is reasonable to believe the theory includes a laborer's rights to their intellectual property.[164]

Additionally, Locke's theory posits that one's "labor" is not restricted to that of physical nature—instead, intellectual labor merits the same protections.[165] Accordingly, the product of a person's intellect is their own, just as any part of their body.[166] Applying Locke's theory and effectively establishing duties for property owners serves a utilitarian purpose, ultimately aiding society.[167] Most intellectual property laws in the United States are based primarily on utilitarian-economic-efficiency justifications.[168]

Further, aside from proposed labor rights, Locke's theory also revolved around the idea that all people possess a "personal identity" comprised of private and personal information inherent to that individual.[169] Under this theory, it is prohibited to collect, access, or retain another's personal information and data without their permission because each person

---

162. *See* Alexander D. Northover, Comment, *"Enough and as Good" in the Intellectual Commons: A Lockean Theory of Copyright and the Merger Doctrine*, 65 EMORY L.J. 1363, 1368 (2016) (citing JOHN LOCKE, SECOND TREATISE OF GOVERNMENT 18 (C.B. McPherson ed., Hackett Publ'g Co. 1980)).

163. *Id.* (quoting LOCKE, *supra* note 162, at 19).

164. *See id.* at 1376.

165. *See* Shlomit Yanisky-Ravid, *The Hidden Though Flourishing Justification of Intellectual Property Laws: Distributive Justice, National Versus International Approaches*, 21 LEWIS & CLARK L. REV. 1, 9 (2017).

166. *Id.*

167. *See* Northover, *supra* note 162, at 1364.

168. *See* Yanisky-Ravid, *supra* note 165, at 4 (first quoting U.S. CONST. art. 1, § 8, cl. 8; and then citing William M. Landes & Richard A. Posner, *An Economic Analysis of Copyright Law*, 18 J. LEGAL STUD. 325, 326 (1989)).

169. Vera Bergelson, *It's Personal but is it Mine? Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379, 420 (2003).

possesses inherent exclusionary rights to their information by virtue of its inherent personal uniqueness.[170] Therefore, an individual's data is arguably an intrinsic part of their existence. Not only should this prevent others from access,[171] but one should be entitled to protect their data as they would their very being.

B. Your Data: Personality & Autonomy

An alternative theoretical justification for an individual's right to intellectual property and data turns on Hegel's Theory of Personality, which posits private property rights based on one's acts upon the property.[172] Importantly, when one creates intellectual property, the individual imbues it with intellectual and emotional components of their personhood; therefore, the originator owns any resultant product—in this case, their data.[173]

Some may argue that "assigning individuals property rights [and attributing basic autonomy] in their personal information" would transform property into a tangible medium, eliminating the "moral advantage" over others seeking their intellectual data.[174] However, physical acts upon inherently "intellectual" property should not render its protections inert; personal information deserves the same deference accorded to the respective owners.[175]

C. A Law & Economics Justification

The Law and Economics theory, a driving institutional approach, currently guides intellectual property laws in the United States.[176] Namely, this theory stresses the promotion of scientific and cultural goods that engender widespread

170. *Id.* at 420–21. The Author compares this to an individual who prohibitively takes a flower from another's garden. *Id.* at 421. The property owner need not perform any action prior to the picking, rather, they already have inherent property rights in the flower. *See id.*

171. *See id.* at 420–21.

172. *See generally* GEORG WILHELM FRIEDRICH HEGEL, HEGEL'S PHILOSOPHY OF RIGHT 40–57 (T. M. Knox Trans., 1942) ("We take possession of a thing . . . by directly grasping it physically, . . . by forming it, and . . . by merely marking it as ours.").

173. *See* Yanisky-Ravid, *supra* note 165, at 9 (citing Margaret Jane Radin, *Property and Personhood*, 34 STAN. L. REV. 957, 986 (1982) (noting that intellectual property and assets that are not replaceable should be more vigorously protected than more fungible assets).

174. Bergelson, *supra* note 169, at 432.

175. *See id.*

176. Yanisky-Ravid, *supra* note 165, at 7.

economic benefits.[177] The goal is to "maximize the total social welfare from an economic perspective."[178] This approach incentivizes technological advancement by creating laws that protect developers from those wishing to copy their work.[179] Although this approach may seem disparate, it can play an integral role in creating the right to data encryption insofar as any new framework must consider the economic ramifications of any new technological regulations or freedoms, consistent with the Law and Economics approach.

D. Consistency & Mirroring Legal Frameworks

A third consideration is to analyze how United States laws have historically treated tangible property.[180] While there are some limitations, United States law has often recognized one's rights to the property in which they infuse labor.[181] Courts have even recognized intellectual property rights in individuals' creations, even where the tangible medium embodying the product belongs to someone else.[182] Accordingly, there are considerable theoretical justifications embodied in established law that support one's right to possess, maintain, and exclude others from their property, as well as the equivalent rights to one's intellectual property and data.

Scholars and legal professionals have proposed theoretical justifications for the individual's right to property for years.[183] This Article does not attempt to present novel justifications for these rights. Instead, this Article asserts that if these justifications exist, accompanying them is an inherent right to protect one's intellectual property and data by any available and appropriate means, including utilization of encryption to defend it from misappropriation, misuse, or merely prying eyes.[184]

---

177. *Id.*
178. *Id.*
179. *Id.*
180. *See* Wendy J. Gordon, *A Property Right in Self-Expression: Equality and Individualism in the Natural Law of Intellectual Property*, 102 YALE L.J. 1533, 1578 (1993).
181. *See id.* at 1579.
182. *See generally* Cohen v. G & M Realty L.P., 320 F. Supp. 3d 421 (E.D.N.Y. 2018) (holding that the Visual Artists Rights Act protected graffiti artists' right to their artwork that is located on another party's real estate property and that the building owner must pay restitution for destroying the artwork).
183. *See* Bergelson, *supra* note 169, at 419–20 (discussing Locke, Bentham, and Hegel's theories of property).
184. From individuals, governments, corporations, or any other entities.

VII. CONCLUSION

Today's world is replete with technology. Our lives are impacted daily by computers, phones, servers, information systems, and the data with which they function. In some way, digital data informs almost every interaction, decision, and experience. While there may exist legitimate concerns other than individual liberties, one's data is of the utmost importance, and must be zealously safeguarded.

Finally, existing justifications, developing laws, and many arguments favor a right to secure digital information. Therefore, this Article posits the necessity to devise a new right to data encryption. This right will require fine-tuning before its implementation. Nonetheless, the narrow but pivotal benefits of the right to data encryption will afford technology users the necessary protections they require. In considering this proposed right's implementation, the United States' legal system must accord proper respect to the growing needs of its citizens in a rapidly evolving technological world.