Washington and Lee Law Review

Volume 72 | Issue 3 Article 12

Summer 6-1-2015

Averting the Inherent Dangers of "Going Dark": Why Congress Must Require a Locked Front Door to Encrypted Data

Geoffrey S. Corn
South Texas College of Law

Averting the Inherent Dangers of "Going Dark": Why Congress Must Require a Locked Front Door to Encrypted Data

Geoffrey S. Corn*

"I don't want a back door . . . I want a front door. And I want the front door to have multiple locks. Big locks."

—*Adm. Michael S. Rogers, Director of the NSA*[1]

I. Introduction

Going dark. Few terms in contemporary national security and crime control parlance better exemplify the friction between individual liberty and collective security. Referring both to data "at rest" and "in motion," the term is most often used to describe the effect of encryption technology embedded in commercially available cell phones and communications technologies that allow individuals to easily and effectively prevent access to their cell phone communications and digitally stored data.[2] While

* Presidential Research Professor of Law, South Texas College of Law; Lieutenant Colonel (Retired), U.S. Army Judge Advocate General's Corps. Prior to joining the faculty at South Texas, Professor Corn served in a variety of military assignments, including as the Army's Senior Law of War Advisor, Supervisory Defense Counsel for the Western United States, Chief of International Law for U.S. Army Europe, and as a Tactical Intelligence Officer in Panama. Professor Corn would like to thank his research assistant, Jennifer Whittington, South Texas College of Law Class of 2016.

1. *See* Ellen Nakashima & Barton Gellman, *As Encryption Spreads, U.S. Grapples with Clash Between Privacy, Security,* WASH. POST (Apr. 10, 2015), http://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html?hpid=z1 (last visited June 20, 2015) (discussing the different interests in the debate over data privacy) (on file with the Washington and Lee Law Review).

2. *See* James B. Comey, Dir., FBI, Remarks at Brookings Institution (Oct. 16, 2014) (explaining the challenge of maintaining national security because of emerging technologies), *available at* http://www.fbi.gov/news/speeches/going-

government officials have decried the problem of "going dark" for several years, their concerns were recently emphasized by Apple and Google's decision to make encryption the default setting on their smartphones. And, unlike earlier encryption capability embedded in cell phones, this type of encryption is not susceptible to "front door" access through the use of encryption keys retained by the cell phone manufacturer and distributor.[3] This unqualified encryption capability is increasingly viewed by democratic governments as a dangerous evolution of technology available to the general public.[4] From a public security perspective, the confluence of pervasive use of cell devices to engage in communication with this encryption creates an unacceptable obstacle to lawful searches and surveillance that are necessary to protect the public from criminal and national security threats.[5]

FBI Director James Comey's comments about the problem of "going dark," given at the Brookings Institute on October 16, 2014,[6] have reignited a debate that many believed was dead at the end of the "crypto-wars" of the 1990s. Since that time, encryption technologies have flourished within the United States and globally, in both the public and private sectors.[7] Nobody, including

---

dark-are-technology-privacy-and-public-safety-on-a-collision-course.

3. *See* Brian Naylor, *Apple Says iOS Encryption Protects Privacy; FBI Raises Crime Fears,* NPR (Oct. 8, 2014, 5:17 PM), http://www.npr.org/blogs/alltechconsidered/2014/10/08/354598527/apple-says-ios-encryption-protects-privacy-fbi-raises-crime-fears (last visited June 20, 2015) (discussing concerns about Apple's policy on data encryption) (on file with the Washington and Lee Law Review).

4. *See* President Barack Obama & Prime Minister David Cameron, Remarks in Joint Press Conference, The White House, Office of the Press Secretary (Jan. 16, 2015) (discussing the potential dangers of data encryption), *available at* https://www.whitehouse.gov/the-press-office/2015/01/16/remarks-president-obama-and-prime-minister-cameron-united-kingdom-joint-; Comey, *supra* note 2 ("[T]he FBI has a sworn duty to keep every American safe from crime and terrorism, and technology has become the tool of choice for some very dangerous people.").

5. *See* Comey, *supra* note 2 (noting the ability to evade law enforcement as data encryption becomes more common).

6. *See id.* (explaining the potential dangers of spreading data encryption).

7. *See Global Encryption Software Market 2019–Incidence of Data Breaches Drives Growth,* PR NEWSWIRE (Mar. 18, 2015), http://www.prnewswire.com/news-releases/global-encryption-software-market-2019---incidence-of-data-breaches-drives-growth-296759501.html (last visited June 20, 2015) (explaining that recent data breaches have motivated organizations to encrypt data) (on file with

Director Comey, would challenge the value of encryption or the essential role it plays in digital security. Indeed, the government regularly encourages and promotes the adoption of strong and well-implemented encryption to protect sensitive data.[8] Director Comey's comments, however, highlighted the continued and evolving danger to the public posed by unlimited and irreversible encryption. The creation of a zone that is essentially immune from government access would undoubtedly promote privacy, but there is no question that it will also promote crime. In fact, as many recent studies have shown, it already has.[9] Police face a real and significant threat that their ability to access evidence, even when armed with a warrant, will continue to decrease in coming years as encryption technologies become stronger and easier to implement. Without legal restrictions, the danger of "going dark" is palpable and must not be ignored.

Civil libertarians see the issue from a completely different perspective. Their focus is not the risk to public security that the government emphasizes, but the risk of abusive government surveillance tactics that erode individual liberty.[10] Citing what

---

the Washington and Lee Law Review).

8. *See* Kara Swisher, *Obama: The Re/Code Interview*, RE/CODE (Feb. 15, 2015), http://recode.net/2015/02/15/white-house-red-chair-obama-meets-swisher/ (last visited June 20, 2015) ("[T]here's no scenario in which we don't want really strong encryption.") (on file with the Washington and Lee Law Review); *Security Tip (ST04-019): Understanding Encryption*, US-CERT, https://www.us-cert.gov/ncas/tips/ST04-019 (last updated Feb. 6, 2013) (last visited June 20, 2015) (explaining how data encryption works) (on file with the Washington and Lee Law Review); *see also, e.g.*, *Smartphone Users Should Be Aware of Malware Targeting Mobile Devices and the Safety Measures to Help Avoid Compromise,* FED. BUREAU OF INVESTIGATION (Oct. 22, 2012), http://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 visited June 20, 2015) (providing advice on how to protect your smartphone from hackers) (on file with the Washington and Lee Law Review).

9. *See* Comey, *supra* note 2 (explaining that the increased use of data encryption has resulted in increased crime); Andy Greenberg, *Over 80 Percent of Dark-Web Visits Relate to Pedophilia, Study Finds*, WIRED (Dec. 30, 2014), http://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/ (last visited June 20, 2015) (explaining that a great deal of anonymous internet traffic is directed at pedophilia-related websites) (on file with the Washington and Lee Law Review).

10. *See* Joshua Kopstein, *The FBI Wants Apple to Make a Defective Phone,* AL JAZEERA (Oct. 24, 2014), http://america.aljazeera.com/opinions/2014/10/fbi-surveillanceappleprivacyencryption.html (last visited June 20, 2015) (discussing

they believe is a consistent pattern of overzealous and unconstitutional government surveillance efforts directed against telephone and computer communications, they applaud the enhanced protection for individual privacy this technology has made the norm and not the exception.[11]

In many ways, the "going dark" debate exemplifies a broader tension that has, since the inception of our nation, animated the line between public security and individual liberty. To facilitate progress in the debate, aides to President Obama are in the midst of preparing a report that will summarize the ways that the administration can bridge the gap between the government and privacy advocates.[12] Finding the point of equilibrium between these two interests was the motivation for protection provided by the Fourth Amendment and the subsequent extension of these protections to the states through the conduit of the Fourteenth Amendment. But these protections are not, and have never been, understood as absolute. Achieving equilibrium between these competing interests also demands recognition that the text of the Fourth Amendment, along with the jurisprudence that has added established meaning to that text, establishes that restrictions on government surveillance are not and cannot be absolute.

The proverbial fulcrum upon which this equilibrium must rest is the test of reasonableness, a concept characterized as the "touchstone" of the Fourth Amendment by the Supreme Court time and again. The notion of an absolute or unqualified barrier to government surveillance is fundamentally inconsistent with this standard of reasonableness, as it would enable activities that endanger the public, immune from lawful government detection. But encryption technology has evolved, and will likely continue to evolve, to enable the average user of personal communication devices to "go dark" with little or no effort.[13] Does this technology

---

the wishes of law enforcement agencies for companies to sell phones with less protected data) (on file with the Washington and Lee Law Review).

11. *See id.* (discussing increased efforts to keep data private).

12. *See* Elise Viebeck, *White House Seeks to Break the Encryption Stalemate,* THE HILL (Apr. 13, 2015), http://thehill.com/policy/cybersecurity/238602-white-house-seeks-to-break-encryption-stalemate (last visited June 20, 2015) (discussing a forthcoming report that details possible approaches law enforcement can take to access private data if necessary for an investigation) (on file with the Washington and Lee Law Review).

13. *See* Comey, *supra* note 2 (discussing the prevalence of data encryption in

shift the fulcrum of the balance of interests at the core of the Fourth Amendment? Is there a net gain to society of adhering to the principles that underlie the Fourth Amendment such that the fulcrum should be reset to its traditional position? If so, should Congress prohibit the sale or dissemination of communications and storage technologies that render court-issued search warrants meaningless? Is there a way to accomplish this without creating an unacceptable level of risk to the privacy of "The People?"

This Essay argues that the answer to this ultimate question is an emphatic yes; that to protect the interests of society, Congress should compel any manufacturer or distributor of communications and storage technologies that offer encryption as part of any product they sell or distribute in the United States to build in a mechanism allowing for lawful government surveillance and searches of the data stored or transmitted over those devices or services. Such access should *not* be through a "back door," but instead through a well-documented and tested "front door" that ensures timely and efficient access to information when lawfully authorized. This Essay acknowledges the privacy interests implicated by this requirement; however it also proposes a novel protective measure to ensure that this requirement will not distort the balance of interests at the core of the Fourth Amendment: bifurcated control of encryption keys. Our proposal is that device manufacturers and communications system developers, whether domestic or foreign, should be encouraged to incorporate strong encryption technologies into their products, but they also should be prohibited from marketing devices or services in the United States that provide unqualified encryption that would prevent lawful access to users' communications and data. Instead, legislation should require manufacturers and developers to create encryption keys that would be bifurcated and placed under the control of the manufacturer and some non-government entity devoted to privacy protection. Government access to the keys would therefore require lawful authorization that must satisfy both entities in control of the keys, either of which would be authorized, pursuant to statute, to challenge the legality of access.

---

technological devices).

II. The Inherent Balance of Fourth Amendment Interests

There are, of course, those who fear that a requirement to preserve even front door access to communications and stored data will also facilitate such access when it is not lawfully authorized or that lawful authorizations will nonetheless permit unjustified intrusions into individual privacy.[14] Essentially, they assert that the government simply cannot be trusted with any ability to intrude on people's privacy, whether authorized or not, and the encryption technologies that make it increasingly easy for individual users to "go dark" are a natural and appropriate response to unacceptable government overreach and intrusions of privacy. Others argue that the preservation of any "door," whether front or back, creates vulnerabilities that cannot be tolerated in a free society.[15]

Unfortunately, this endorsement of impenetrable encryption reflects a dangerous distortion of the balance between government surveillance authority and individual liberty central to the Fourth Amendment. Nowhere are the competing interests of collective societal security and individual liberty more apparent than in the text of that Amendment. There is no question that the Fourth Amendment *restricted* the government's surveillance authority in the interests of protecting individual privacy and liberty. Nothing, however, in the text, history, or subsequent interpretation of the Fourth Amendment supports the conclusion that it provides an absolute barrier to such surveillance. Instead, balance is the operative word: the Fourth Amendment also acknowledged that the people must be subjected to searches. So long as that search is

---

14. *See* Kopstein, *supra* note 10 (discussing mistrust of government intrusions).

15. *See, e.g.*, Nakashima & Gellman, *supra* note 1 (""The basic question is, is it possible to design a completely secure system' to hold a master key available to the U.S. government but not adversaries . . . . 'There's no way to do this where you don't have unintentional vulnerabilities.'"); Carrie Johnson, *Privacy Advocates Don't Buy FBI's Warning About Encryption Practices*, NPR (Oct. 17, 2014), http://www.npr.org/2014/10/17/356869566/privacy-advocates-don-t-buy-fbi-s-warning-about-encryption-practices (last visited June 20, 2015) ("[I]f these companies are delivering end-to-end encrypted communications, the only logical way to provide law enforcement access is to escrow a key. And if the keys are there, whether they are in law enforcement hands, a third party or in the company's hands, people will try and steal them.") (on file with the Washington and Lee Law Review).

reasonable within the meaning of the Amendment, it is lawful and permissible. In short, the people have never had an absolute and unqualified right to privacy but instead a right to be secure against *unreasonable* government intrusions into those places and things protected by the Fourth Amendment.

The Supreme Court has consistently emphasized the importance of this balance and that, when assessing the reasonableness of government surveillance, it is necessary to acknowledge the government's interest in effective law enforcement.[16] One need not dig deep to identify this vein of analysis in many seminal Fourth Amendment decisions. For example, in *Schneckloth v. Bustamonte*,[17] the Court addressed the validity of consent obtained without providing notice of a right to refuse the officer's request.[18] The Court endorsed a totality of the circumstances test for assessing the validity of consent and rejected the Ninth Circuit's ruling that notice of the right to decline consent is a necessary requirement.[19] In the opinion, the Court emphasized the importance of consent, not in abstract terms, but in direct connection with the function of law enforcement—solving crimes:

> [I]n situations where the police have some evidence of illicit activity, but lack probable cause to arrest or search, a search authorized by a valid consent may be the only means of obtaining important and reliable evidence . . . a search pursuant to consent may result in considerably less inconvenience for the subject of the search, and, properly conducted, is a constitutionally permissible and wholly legitimate aspect of effective police activity.[20]

Later in the opinion, the Court again emphasized the link between consent and the function of law enforcement, noting that, "the community has a real interest in encouraging consent, for the

---

16. *See* Schneckloth v. Bustamonte, 412 U.S. 218, 225 (1973) (discussing the need for police questioning); Smith v. Maryland, 442 U.S. 735, 735 (1979) (noting that the expectation of privacy must be weighed against the government action).

17. 412 U.S. 218 (1973).

18. *See id.* at 223 (discussing voluntariness in responding to questions by law enforcement).

19. *See id.* at 225–30 (noting that officers are not required to inform individuals of the right to decline consent).

20. *Id.* at 227–28.

resulting search may yield necessary evidence for the solution and prosecution of crime . . . ."[21]

Of course, issues related to encryption of communications and stored data do not implicate consent. However, like consent, they clearly implicate the balance between the need to enable effective government surveillance and individual privacy. And there is perhaps an even more important link to *Bustamonte*: overly restrictive standards that frustrate legitimate law enforcement surveillance efforts conflict with the Fourth Amendment's core objective. Indeed, this was the primary basis for the Court's rejection of the Ninth Circuit's conclusion that notice of a right to decline consent was a dispositive requirement for validity. As the Court noted,

> The problem of reconciling the recognized legitimacy of consent searches with the requirement that they be free from any aspect of official coercion cannot be resolved by any infallible touchstone. To approve such searches without the most careful scrutiny would sanction the possibility of official coercion; to place artificial restrictions upon such searches would jeopardize their basic validity. Just as was true with confessions, the requirement of a "voluntary" consent reflects a fair accommodation of the constitutional requirements involved.[22]

Allowing device manufacturers and communications service providers to embed technologies in their products that make it impossible for the government to gain access to an individual's data is the surveillance analogue to the "artificial restriction" on lawful government activity that the Court condemned in *Bustamonte*.[23] In fact, such encryption is even more incompatible with the Fourth Amendment's inherent balance because unlimited use of encryption technology is not intended to impose a "restriction" on lawful surveillance—it is intended to impose a complete prohibition.

Concededly, prohibiting this type of encryption will force individuals to assume some increased risk of unauthorized access. Indeed, this seems to be the principal argument in support of both

---

21. *Id.* at 243.

22. *Id.* at 229.

23. *See id.* (discussing the dangers of placing unnecessary restrictions on police searches).

the necessity and legitimacy of such encryption.[24] But the risk that the government will abuse its authority and engage in unlawful surveillance cannot justify a complete barrier to *lawful* surveillance. Indeed, the Fourth Amendment itself tolerates such risk by allowing for lawful government searches and surveillance in the first place.

Accordingly, addressing the validity of "going dark" encryption should not focus on whether prohibiting such encryption creates a risk of unlawful government access to information but instead whether the risk it creates is necessary to preserve the inherent balance of Fourth Amendment interests. Moreover, the weight of the risk must be evaluated on the basis of how much it can be mitigated through technological and legislative solutions, allowing for a meaningful cost-risk analysis. Indeed, this more precise risk assessment was endorsed by none other than Justice Marshall in his dissenting opinion in *Smith v. Maryland*,[25] ironically the decision that provides the foundation for almost all arguments in support of government collection of communications metadata. In *Smith*, the Court held that there is no reasonable expectation of privacy in the numbers dialed from a private telephone in an individual's home because the numbers are divulged to the third party phone company.[26] Accordingly, government access to those numbers in no way implicated the protections of the Fourth Amendment.[27]

Justice Marshall rejected this conclusion. In his view, the "exposed to a third party" touchstone for assessing the reasonableness of an expectation of privacy, and the accordant applicability of the Fourth Amendment, was invalid.[28] Instead, Justice Marshall believed that the nature of functioning in a free society necessitated its citizens to divulge certain information—in

---

24. *See* Kopstein, *supra* note 10 (discussing the benefits of data encryption).

25. *See* Smith v. Maryland, 422 U.S. 735, 735 (1979) (weighing the risk of government interference).

26. *See id.* at 745–46 (explaining that privacy expectations should be lower because the information has already been given to a third party).

27. See *id.* (discussing the fact that government access to that information does not unreasonably interfere with privacy expectations).

28. *See id.* at 748–50 (Marshall, J., dissenting) (arguing against the third-party doctrine in the majority opinion).

this case phone numbers.[29] Thus, Justice Marshall rejected the conclusion that an individual forfeited an expectation of privacy in information simply by disclosing it to a third party.[30] Rather, he argued, the real test was not "whether privacy expectations are legitimate [based] on the risks an individual can be presumed to accept when imparting information to third parties, but on the risks he should be forced to assume in a free and open society."[31]

Justice Marshall's view of the "Third Party Doctrine" seems to be gaining new momentum as courts struggle to apply the Fourth Amendment's warrant requirements to increasingly ubiquitous digital storage devices. Judges across the United States, from magistrates to the Supreme Court, are becoming increasingly persuaded that somehow the dynamics have shifted as a result of these "super-storage" containers. This struggle was reflected in the Supreme Court's recent decisions in *United States v. Jones*[32] and *Riley v. California*.[33] Justice Sotomayor's concurrence reflected this struggle—arguing that what society is willing to accept as a reasonable expectation of privacy should turn not so much on the information an individual exposes to the public but instead on whether the collection of that information is so extensive as to "alter the relationship between citizen and government in a way that is inimical to democratic society."[34] Thus, Justice Sotomayor seeks to revive Justice Marshall's view when arguing that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[35]

---

29. *See id.* (noting that calling a phone number should not kill any expectation of privacy).

30. *See id.* (disagreeing with the third-party doctrine that the Court adopted).

31. *Id.* at 750.

32. 132 S. Ct. 945, 946 (2012) (introducing the difficulty in applying existing doctrine to emerging technologies).

33. 134 S. Ct. 2473, 2482 (2014) (discussing the reasonableness of searching information stored in a cell phone without a warrant).

34. *Jones*, 132 S. Ct. at 956 (citing United States v. Cuevas–Perez, 640 F.3d 272, 285 (7th Cir. 2011)).

35. *Id.* at 957 ("I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection." (citing Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting) ("Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or

This theme continues in *Riley*, where the Supreme Court considered whether the police could search a cellular telephone incident to arrest.[36] The Court's opinion in *Riley,* which overturned well-established precedents, hinged entirely on the fact that such a great deal of data could be stored in a modern smartphone.[37] Thus, Chief Justice Roberts concluded, such devices are simply quantitatively and "qualitatively different."[38]

Ironically, Justice Marshall's more restrictive standard for assessing applicability of Fourth Amendment protections provides a compelling justification for restricting "going dark" encryption. Prohibiting such unlimited encryption would, to some extent, increase the risk of unlawful government access (although, as explained below, probably not nearly as much as many privacy advocates would have the public believe). But this risk is inherent

---

phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes.")))).

36. *See Riley*, 134 S. Ct. at 2480 (questioning the constitutionality of warrantless cell phone searches).

37. *See id.* at 2489 (considering the storage capability of current technology).

38. *Id*. at 2490. Some courts and scholars pushed this argument further, asserting that even searches conducted pursuant to warrants should be strictly constrained in their scope when applied to digital devices due to the enormous amounts of data those devices can store. *See, e.g.*, United States v. Comprehensive Drug Testing, Inc.*,* 579 F.3d 989, 994 (9th Cir. 2009), *opinion revised and superseded*, 621 F.3d 1162 (9th Cir. 2010) (discussing the need to protect privacy interests); *see also In re* Search of Apple iPhone, 31 F. Supp. 3d 159, 160 (D.D.C. 2014) (denying a search warrant to search an iPhone); *In re* Search of Black iPhone, 27 F. Supp. 3d 74, 78 (D.D.C. 2014) (discussing the risk of the government gaining access to too much private information); *In re* Search of Odys Loox Plus Tablet, 28 F. Supp. 3d 40, 44–46 (D.D.C. 2014) (discussing issues that arise from a search warrant request's lack of clarity in how law enforcement will search the cell phone); *In re* The Search of premises known as: a Nextel Cellular Telephone, No. 14–MJ–8005–DJW, 2014 WL 2898262, at *3–7 (D. Kan. June 26, 2014) (denying a search warrant because the application failed to meet the particularity requirement). Those arguing that digital searches are so different as to require entirely new protocols to control searches seem to believe that the Framers of the Constitution could never have imagined allowing searches of containers that could hold so much personal information. Yet that is exactly what the Framers contemplated when they made abundantly clear that the government should have the authority to search homes—the most sacrosanct of all protected areas. One could argue that the "quantitative and qualitative" differences of modern electronic devices is that they compile much more information than would ever have occurred in the eighteenth century. While this is true, we should also recall that polymaths like George Washington, Thomas Jefferson, and James Madison were notoriously meticulous in documenting and storing their thoughts, communications, and even business records in their homes.

in all government search and surveillance capabilities and is tolerated by the Fourth Amendment. More importantly, this is a risk that members of a free society must accept as a necessary cost to protecting the broader societal interest in facilitating lawful access to evidence. In contrast, preventing access altogether would not only protect individuals from unreasonable searches, but also would protect them from *any* search, thereby frustrating the legitimate governmental and societal interest in discovering crime and protecting national security. And this interest is far from speculative.

Allowing the continued development and use of "going dark" encryption will ultimately distort the balance at the core of the Fourth Amendment. Preserving that balance necessitates a fundamentally different approach: the preservation of "front door" access with a carefully constructed mechanism to guard that front door against unlawful entry. Such a balanced approach is both necessary and feasible.

III. Front Door Access and the "Split Key" Mechanism

Many critics of both "going dark" and efforts to restrict such encryption address the issue through extremes. On one end of the spectrum, advocates for privacy rights emphasize the risk that government collusion with cell device manufacturers will make access to encryption keys too easy, leading to inevitable abuse.[39] On the other end of the spectrum, advocates for public and national security emphasize the dangers of keyless encryption and how that danger necessitates government access to manufacturer encryption keys.[40]

---

39. *See* Mike Masnick, *Everybody Knows FBI Director James Comey Is Wrong About Encryption, Even the FBI*, TECHDIRT (Oct. 20, 2014, 10:22 AM), https://www.techdirt.com/articles/20141019/07115528878/everybody-knows-fbi-director-james-comey-is-wrong-about-encryption-even-fbi.shtml (last visited June 20, 2015) (discussing the current state of data encryption) (on file with the Washington and Lee Law Review).

40. *See* Eric Chabrow, *Obama Sees Need for Encryption Backdoor,* BANK INFO SECURITY (Jan. 16, 2015), http://www.bankinfosecurity.com/cameron-obama-a-7809/op-1 (last visited June 20, 2015) (explaining a few of the different approaches to allowing government access of encrypted information) (on file with the Washington and Lee Law Review).

There is, however, a solution to this problem that, like the Fourth Amendment itself, strikes a credible balance between these two extremes: a "split key" approach. Under this approach, to protect the government's interest in lawful access to encrypted data, manufacturers would be required, by statute, to preserve encryption keys for the devices and services they produce and distribute in the United States. To mitigate the risk of unlawful government access as the result of collusion with manufacturers or the abuse of the manufacturers themselves, these keys would be "split" and retained by two (or more) distinct entities: the manufacturer and a privacy rights organization.

The advantages of this "split key" approach are obvious. Unlike "going dark" encryption, the government's interest in efficient lawful access to encrypted data would be preserved. By splitting control of the encryption key between two entities—one of which would neither be susceptible to government pressure nor profit motives, but instead devoted to protecting the privacy interests of the public—the risk of unlawful government access would be substantially reduced.

Such an approach is obviously contrary to the objectives of some privacy advocates, most notably those who have launched a series of retorts intent on snuffing out the development of mechanisms to preserve efficient lawful access to cell data.[41] The polemic aims to discredit the very concept of allowing any government access whatsoever to encrypted data and communications, suggesting that such access can only be achieved by building defects into the encryption.[42] These opponents frame efforts to preserve such access as a call for the creation of "back doors" that can be exploited by the United States and any other government.[43] They argue that the creation of back doors will introduce unacceptable vulnerabilities in products and systems[44]

---

41. *See With Liberty to Monitor All,* HUM. RTS. WATCH (July 28, 2014), http://www.hrw.org/node/127362/section/2 (last visited June 20, 2015) (providing a summary of a 120-page report that "documents how government surveillance and secrecy are undermining press freedom, the public's right to information, and the right to counsel, all human rights essential to a healthy democracy") (on file with the Washington and Lee Law Review).

42. *See id.* (opposing any changes that would make data less secure).

43. *See id.* (same).

44. Some have argued that the creation of additional encryption keys will be an attractive target for hackers no matter where they are stored. While that is

and point to examples where, in the past, such vulnerabilities have been exploited by hackers.[45]

To be clear, this "split key" proposal is not a subterfuge method of creating "back door" access to data. It, like Director Comey, seeks to achieve preservation of "front door" access to encrypted communications. This might seem like a minor distinction, but it is not, as those who have misrepresented Comey's comments understand perfectly. Unlike a "back door," which generally refers to an undisclosed vulnerability in an application or device, a front door is a well-documented and clear mechanism for both encrypting and decrypting data, whether it be data in motion (communications) or at rest (stored data). To be secure, encryption should be subject to rigorous testing. Thus, its presence should be open to the public and available for attack, both in laboratories and in the real world. This is the only way to truly evaluate the trustworthiness of encryption, with vulnerabilities being corrected as they are discovered, to constantly strengthen the protocol and its implementation. Essentially, a front door is the digital

---

true, it must be acknowledged that hackers, like all logical actors, recognize that a chain is only as strong as its weakest link. Thus, hackers generally seek the path of least resistance to achieve their goals. It would generally be much easier for a hacker to compromise a user's device through a Trojan horse or to obtain their credentials through social engineering than it would be to hack into two or more well protected systems. Moreover, despite modern society's obsession with connectivity, nothing requires a database maintaining encryption keys to be connected to the Internet. Thus, such a database could be immensely more secure than encryption keys or passwords found on users' devices.

45. *See* Johnson, *supra* note 15 (noting that fears about data insecurity are valid "since foreign governments have already found a way to hack into major American tech companies"); The Lawfare Podcast, Episode #98: Chris Soghoian Responds to FBI Director James Comey LAWFARE BLOG (Nov. 1, 2014), http://www.lawfareblog.com/lawfare-podcast-episode-98-chris-soghoian-responds-fbi-director-james-comey (last visited June 20, 2015) (discussing potential problems with weak data security) (on file with the Washington and Lee Law Review). The Athens Affair, cited by Soghoian in this podcast, is probably the most frequently referenced example of the danger of creating "back doors" in communications networks. It is, however, a poor example that speaks more to the need for solid network security than it does to the creation of back doors. For an explanation of how Vodafone's failure to purchase and install Ericsson's Intercept Management System allowed this hack to occur, see 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), http://spectrum.ieee.org/telecom/security/the-athens-affair (last visited June 20, 2015) (discussing a major hack of cell phone data in Greece) (on file with the Washington and Lee Law Review).

equivalent of a big, ingeniously engineered lock on the only entrance to an otherwise secure building. It is a lock that has been tested by every available lock picker and found to be secure, with any identified weaknesses being constantly fixed. Such a lock is always superior to a secret entrance in the rear of a building.

When presented with the option of using the front door versus the back door, law enforcement will always choose the former, and nobody is suggesting that there should be any imperfections built into the front door lock. The only question is: Who should have access to the key, and under what circumstances? One could imagine leaving the key to such a lock in the hands of the manufacturer, the police, or even locked inside another container with a similar lock. All of these scenarios carry different, but manageable, risks. They are also available just as much in the digital world as the real world—in fact more so, as encryption likely is stronger than the most ingenious physical lock ever created.

There is no reason, as is often assumed, that the key to the lock must be placed solely in the hands of the government or the manufacturer, both of which could be motivated by perverse incentives and thereby present risks, as Justice Marshall might argue, that are unacceptable for members of a free society. The split key model mitigates this risk and allows for the preservation of secure, timely, and efficient front door access to evidence when lawfully authorized; splitting the key to provide that access will align the inherent risk of improper access with what should be demanded of a free society.

IV. Splitting the Key

The use of split key encryption to lock access to data significantly mitigates the concern that a duplicate or escrow key will be abused. An encryption key itself can not only be split into discrete parts and stored separately; it can be encapsulated within other "containers" of encrypted data.[46] Each container can be placed in the possession of another entity, requiring cooperation by two or more entities to unlock the series of keys to decrypt the

46. *See supra* Part III (introducing the split key approach and its advantages).

cipher text into plain text[47]. Thus, for example, the manufacturer of a device could hold one portion of the key, or a key to an encapsulated container.[48] A privacy group could hold another key.[49] Only by combining all parts of the key could the cipher text be returned to plain text.[50] If and when the government sought the use of the encryption key, it would bear the burden to satisfy both custodians that access is authorized by law, in most cases as the result of a lawful order. Each custodian would then be in a position to assess the legal basis and contest the order if it believed the access to be improper. Thus, only when both custodians validated the legal basis for access, each of which approaching the question with differing interests, would decryption occur.[51] This split key option preserves privacy, security, and the government's ability to obtain evidence when authorized.

Implementing this split key approach would necessitate a statutory mandate to create, split, and retain encryption keys. Imposition of such a mandate is well within the authority of the federal government as an exercise of its regulation of interstate commerce and communications.[52] A closely related example of such a mandate can be found in the Communications Assistance for Law Enforcement Act (CALEA).[53] While this statute does not require decryption, it does reflect the logical balance between privacy and public security by imposing an obligation on telecommunication providers to build into their systems lawful intercept capabilities. According to a Congressional Research Service report on CALEA:

---

47. *See supra* Part III (explaining what split key encryption may look like).

48. *See supra* Part III (articulating an approach that affords manufacturers autonomy while ensuring their accountability).

49. If Congress so desired, it could place additional keys, or portions of keys, in the hands of other entities—for example, the Administrative Office of the United States Courts or an ombudsman.

50. *See supra* Part III (explaining how the split key model allows for secure, timely, and efficient access to encrypted data).

51. *See supra* Part III (arguing that splitting control of the encryption key between two or more entities with diverging interests would substantially reduce the risk of unlawful government access to encrypted data).

52. *See infra* notes 58–61 and accompanying text (analogizing to the Communications Assistance for Law Enforcement Act as a basis for authority to mandate a split key approach to data encryption).

53. 47 U.S.C. §§ 1001–1010 (2012).

> CALEA is intended to preserve the ability of law enforcement officials to conduct electronic surveillance effectively and efficiently, despite the deployment of new digital technologies and wireless services by the telecommunications industry. CALEA requires telecommunications carriers to modify their equipment, facilities, and services to ensure that they are able to comply with authorized electronic surveillance.[54]

The same report also emphasizes that CALEA was never intended to expand law enforcement surveillance authority, but instead:

> [O]nly to ensure that after law enforcement obtains the appropriate legal authority, carriers will have the necessary capabilities and sufficient capacity to assist law enforcement in conducting digital electronic surveillance regardless of the specific telecommunications systems or services deployed.[55]

For this purpose, the statute requires telecommunication providers to be able to respond expeditiously to government surveillance orders, including the requirement to "consult with telecommunications equipment manufacturers to develop equipment necessary to comply with the capability and capacity requirements identified by the FBI."[56]

But CALEA also offers the type of safeguards a split-key decryption requirement would incorporate. First, it requires telecommunications carriers "to ensure that any interception of communications or access to call-identifying information that is conducted within their premises can only be done with a court order."[57] Second, it provides for a certain degree of execution oversight, in that it also requires the affirmative intervention of an individual officer or employee of the carrier acting in accordance with regulations prescribed by the Federal Communications Commission.[58]

CALEA is a useful model for the split-key decryption statute that would facilitate lawful access to communications and stored

---

54. PATRICIA MOLONEY FIGLIOLA, CONG. RESEARCH SERV., RL30677, DIGITAL SURVEILLANCE: THE COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT 2 (2007), http://fas.org/sgp/crs/intel/RL30 677.pdf.

55. *Id.* at 3.

56. *Id*.

57. *Id.*

58. *Id.*

data.[59] Like CALEA, the split-key option reflects a compromise between public security and individual privacy, ensuring lawful access to data while mitigating the risk of unlawful access or investigatory overreach.[60] And, like CALEA, it reflects the reality that the risk of improper access resulting from the requirement is within the range of risk necessary to further the legitimate public safety and national security interests related to surveillance.[61] A clear and simple mandate to develop and maintain split encryption keys and to include a provision that provides standing to the custodians of the split encryption keys to enable them to challenge the legality of any access request will produce an analogous balance in the realm of encrypted data.

V. Responding to the Inevitable Criticisms

Like CALEA, a statutory obligation along the lines proposed herein will inevitably trigger criticisms and generate concerns.[62] One obvious criticism is that the creation of an escrow key or the maintenance of a duplicate key by a manufacturer would introduce an unacceptable risk of compromise for the device.[63] This argument presupposes that the risk is significant, that the costs of its exploitation are large, and that the benefit is not worth the risk. Yet manufacturers, product developers, service providers, and users constantly introduce such risks. Nearly every feature or bit of code added to a device introduces a risk, some greater than others. The vulnerabilities that have been introduced to computers by software such as Flash, ActiveX controls, Java, and web

59. *See supra* notes 53–54 and accompanying text (explaining that CALEA provides a closely related example for such a mandate).

60. *See supra* notes 53–54 and accompanying text (noting the balance struck between privacy and public security by CALEA).

61. *See supra* Part III (noting that the split key approach better aligns the inherent risk of improper access with the necessity of protecting the broader societal interest in facilitating lawful access to evidence).

62. *See supra* notes 41–45 and accompanying text (noting that criticisms stem from concern over unlawful facilitation of access to communication and the potential for unjustified intrusions into individual privacy even when communications are lawfully accessed).

63. *See supra* notes 15, 39–40 and accompanying text (noting that opponents frame efforts to preserve such access as a call for the creation of easily exploitable "back doors").

browsers are well documented.[64] The ubiquitous SQL database, while extremely effective at helping web designers create effective data driven websites, is notorious for its vulnerability to SQL injection attacks.[65] Adding microphones to electronic devices opened the door to aural interceptions.[66] Similarly, the introduction of cameras has resulted in unauthorized video surveillance of users.[67] Consumers accept all of these risks, however, because we, as individual users and as a society, have concluded that they are worth the cost.

Some will inevitably argue that no new possible vulnerabilities should be introduced into devices to allow the government to execute reasonable, and therefore lawful, searches for unique and otherwise unavailable evidence. However, this argument implicitly asserts that such a feature is either of no value or merely insignificant value to society. Herein lies the Achilles' heel to opponents of mandated front-door access: the conclusion is entirely at odds with the inherent balance between individual liberty and collective security central to the Fourth Amendment itself.[68] Nor should lawmakers be deluded into believing that the

---

64. *See, e.g.*, Ed Bott, *Microsoft to Block Outdated Java Versions in Internet Explorer,* ZDNET.COM (Aug. 6, 2014, 11:54 PM), http://www.zdnet.com/article/microsoft-to-block-outdated-java-versions-in-internet-explorer/ (last visited June 18, 2015) (noting that such software, while easily accessible and useful, can be easily used against users in potentially dangerous ways) (on file with the Washington and Lee Law Review).

65. *See* Gery Menegaz, *SQL Injection Attack: What It Is and How to Prevent It,* ZDNET.COM (July 13, 2012, 12:13 PM), http://www.zdnet.com/article/sql-injection-attack-what-is-it-and-how-to-prevent-it/ (last visited June 18, 2015) (explaining why SQL Injection attacks are so common) (on file with the Washington and Lee Law Review).

66. *See* Laurent Simon & Ross Anderson, *PIN Skimmer: Inferring PINs Through the Camera and Microphone*, *in* PROCEEDINGS OF THE THIRD ACM WORKSHOP ON SECURITY AND PRIVACY IN SMARTPHONES & MOBILE DEVICES 67 (Nov. 8, 2013), http://www.cl.cam.ac.uk/~rja14/Papers/pinskimmer_spsm13.pdf (discussing how phone cameras, microphones, and other sensors can be used as powerful, cheap, and convenient spying tools).

67. *See* Rebecca Abrahams & Stephen Bryen, *Your Computer and Phone Cameras Are On—Beware!*, HUFFINGTON POST (July 27, 2014, 5:59 AM), http://www.huffingtonpost.com/rebecca-abrahams/your-computer--phone-came_b_5398896.html (last visited June 18, 2015) (noting that spying through smartphone cameras, computer webcams, laptops, and tablets is widespread practice by various governments) (on file with the Washington and Lee Law Review).

68. *See supra* Part II (maintaining that allowing for unqualified absolute

currently existing vulnerabilities that we live with on a daily basis are less significant in scope than the possibility of obtaining complete access to the encrypted contents of a device. Various malware variants that are so widespread as to be almost omnipresent in our online community achieve just such access through what would seem like minor cracks in the defense of systems.[69]

One example is the Zeus malware strain, which has been tied to the unlawful online theft of hundreds of millions of dollars from United States companies and citizens and gives its operator complete access to and control over any computer it infects.[70] It can be installed on a machine through the simple mistake of viewing an infected website or email, or clicking on an otherwise innocuous link.[71] The malware is designed to not only bypass malware detection software, but also to *deactivate* the software's ability to detect it.[72] Zeus and the many other variants of malware that are freely available to purchasers on dark-net websites and forums are responsible for the theft of funds from countless online bank accounts (the credentials having been stolen by the malware's key-logger features), the theft of credit card information, and innumerable personal identifiers.[73]

---

encryption will ultimately distort the balance at the core of the Fourth Amendment).

69. *See Malware Creation Increasing, Trojans Most Popular Attack,* TREND MICRO (Nov. 28, 2014), http://blog.trendmicro.com/malware-creation-increasing-trojans-popular-attack/ (last visited June 18, 2015) (noting that malware creation "has been growing at an unprecedented rate" and the global infection ratio has been increasing) (on file with the Washington and Lee Law Review).

70. *See GameOver Zeus Botnet Disrupted,* FBI (June 2, 2014), http://www.fbi.gov/news/stories/2014/june/gameover-zeus-botnet-disrupted (last visited June 18, 2015) (announcing that the collaborative effort among international partners to disrupt GameOver Zeus and Cryptolocker have proven successful, and that "significant progress has been made in remediating computers infected with the GameOver Zeus") (on file with the Washington and Lee Law Review).

71. *See id.* (noting that the infection was predominantly spread through spam e-mail or phishing messages).

72. *See id.* (noting that the malware was able to download and install additional malware, which was then used to extract banking credentials and facilitate the illegal withdrawal of funds from individuals and businesses).

73. *See id.* ("In the case of GameOver Zeus, its primary purpose is to capture banking credentials from infected computers, then use those credentials to initiate or re-direct wire transfers to accounts overseas that are controlled by the

Critics of requiring preservation of "front-door access" will likely also argue that society will be better served by pursuing the unrestrained development of encryption technology. These two approaches are not, however, incompatible. However, it is both naïve and dangerous to fail to recognize—and account for—the reality that some of these advances bring with them risks that must be managed at a societal level. Ultimately, individual choices or actions will not be sufficient to diminish or minimize such risks. Some suggest that any restriction on the evolution of encryption technology is the digital equivalent to prohibiting development of the automobile. This type of hyperbole distorts the issue. If there is an analogue, it is more appropriately characterized as simply requiring the development of safety mechanisms as the automobile evolves. Industry is today capable of this type of more cautious and responsible development of encryption technology. Few could reasonably argue that it would have been more efficient to design the automobile with safety features at the outset, rather than trying to cobble together solutions to the dangers they impose at a later date. This is the opportunity available in relation to encryption.

Is there precedent for using a split key approach to encryption? Absolutely. It may surprise some to learn that the security of the entire Internet domain system is, essentially, being protected by a split key approach.[74]

Why, however, should the government interfere with the free-market evolution of encryption technology, imposing a requirement to incorporate and preserve "front door access" to data? The answer is twofold. First, the market is producing an

---

criminals. Losses attributable to GameOver Zeus are estimated to be more than $100 million.").

74. *See* Adam Hadhazy, *Internet 'Key Holders' Are Insurance Against Cyber Attack*, LIVESCIENCE (July 29, 2010, 5:48 AM), http://www.livescience.com/6791-internet-key-holders-insurance-cyber-attack.html (last visited June 18, 2015) (on file with the Washington and Lee Law Review)

> At least five key-holding members of this fellowship would have to meet at a secure data center in the United States to reboot this so-called Domain Name System Security Extensions (DNSSEC) in case of a very unlikely system collapse. 'If you round up five of these guys, they can decrypt [the root key] should the West Coast fall in the water and the East Coast get hit by a nuclear bomb,' Richard Lamb, program manager for DNSSEC at ICANN, told TechNewsDaily.

outcome in conflict with the Fourth Amendment's central and essential balance of interests.[75] Second, the market-driven evolution of encryption technology distorts this balance because the costs of the dangers imposed by the technology are externalized to society, rather than internalized by the manufacturer or individual users.[76] When the costs of market-driven development—in this case, frustration of lawful government surveillance efforts—are so widespread among society, the market impact is diluted and cannot produce a rational influence. It is precisely in such situations that governmental action is required to avoid the common pool problem—the "race to the bottom" as described in the law and economics theory.

Arguably, the market would drive manufacturers to include such "front door access" features if doing so was perceived by the consumer to be in her best interest.[77] But because the vast majority of users will be more interested in the security of their data than in the ability of the government to gain access to that data in the course of lawful surveillance activities, the societal interest is poorly aligned with market forces.[78] Only when individuals are directly affected by the inability of the government to access such information will they have any motivation to complain. This may result in the occasional article or outcry by the victim of a crime, but it is unlikely to shift the balance of public opinion, or more importantly, to make such an impact on the sales of a given product as to alter market oriented encryption development. This is true despite the fact that the cost to the victim will likely be

---

75. *See supra* Part II (noting that an absolute barrier to government surveillance is fundamentally inconsistent with the reasonableness standard of the Fourth Amendment).

76. *See supra* Part II (noting that preventing access altogether would frustrate the legitimate governmental interest in discovering crime and protecting national security).

77. *See supra* Part IV (noting that such drivers would reflect a logical balance between privacy and public security by way of imposition of an obligation on telecommunication providers to build lawful intercept capabilities into their systems).

78. *See* Kevin Poulson, *Apple's iPhone Encryption Technology Is a Godsend, Even If Cops Hate It,* WIRED (Oct. 8, 2014, 6:30 AM), http://www.wired.com/2014/10/golden-key/ (last visited June 18, 2015) ("With an eye to market demand, the company has taken a bold step to the side of privacy, making strong crypto the default for the wealth of personal information stored on the iPhone.") (on file with the Washington and Lee Law Review).

exponentially greater than the benefits to users of the device lacking the feature. Thus, legislation or government regulation is appropriate to ensure that such features are included.

None of these considerations will persuade everyone that mandated front door access is a necessary measure to preserve a credible and effective balance between individual liberty and public security.[79] There will always be critics who fear that no matter how carefully the law controls access to an encryption key to the front door, it will be abused and result in unauthorized access.[80] Others are concerned that even authorized use of the key, while lawful, will nonetheless permit unjustified intrusions into individual privacy.[81] These fears, however, are inherent in any government search and surveillance capability and have been historically managed effectively. Thus, the first of these fears is fairly easily managed. As for the second, it is the People—represented by Congress and the state legislatures and limited by the Constitution—that decide when privacy rights trump the government's need to obtain evidence. As described above, in United States jurisprudence, this balance has consistently weighed in favor of government access to evidence; nothing about encryption should change this conclusion.

VI. Conclusion

The risks related to "going dark" are real. When the President of the United States,[82] the Prime Minister of the United

79. *See supra* Part II (conceding that there are those who fear that a requirement to preserve even front door access to communications and stored data will also facilitate such access when it is not lawfully authorized).

80. *See supra* Part II (noting that these same skeptics will attack even lawful authorizations for access to encrypted data as nonetheless permitting unjustified intrusions into individual privacy).

81. *See supra* notes 41–45 and accompanying text (noting that such critics assert that government simply cannot be trusted with any ability to intrude on people's privacy, whether authorized or not).

82. Nakashima & Gellman, *supra* note 1.

Kingdom,[83] and the Director of the FBI[84] all publicly express deep concerns about how this phenomenon will endanger their respective nations, it is difficult to ignore. Today, encryption technologies that are making it increasingly easy for individual users to prevent even lawful government access to potentially vital information related to crimes or other national security threats. This evolution of individual encryption capabilities represents a fundamental distortion of the balance between government surveillance authority and individual liberty central to the Fourth Amendment. And balance is the operative word. The right of the people to be secure against *unreasonable* government intrusions into those places and things protected by the Fourth Amendment must be vehemently protected. Reasonable searches, however, should not only be permitted, but they should be mandated where necessary.

Congress has the authority to ensure that such searches are possible. While some argue that this could cause American manufacturers to suffer, saddled as they will appear to be by the "Snowden Effect," the rules will apply equally to any manufacturer that wishes to do business in the United States. Considering that the United States economy is the largest in the world, it is highly unlikely that foreign manufacturers will forego access to its market to avoid having to create CALEA-like solutions to allow for lawful access to encrypted data. Just as foreign cellular telephone providers, such as T-Mobile, are active in the United States, so too will foreign device manufacturers and other communications services adjust their technology to comply with our laws and regulations. This will put American and foreign companies on an equal playing field while encouraging ingenuity and competition. Most importantly, "the right of the people to be secure in their persons, houses, papers, and effects" will be protected not only "against unreasonable searches and seizures,"[85] but also against

83. James Ball, *Cameron Wants to Ban Encryption—He Can Say Goodbye to Digital Britain,* THE GUARDIAN (Jan. 13, 2015), http://www.theguardian.com/commentisfree/2015/jan/13/cameron-ban-encryption-digital-britain-online-shopping-banking-messaging-terror (last visited July 10, 2015) (discussing David Cameron's views on data encryption) (on file with the Washington and Lee Law Review).

84. Comey, *supra* note 2.

85. U.S. CONST. amend. IV.

attacks by criminals and terrorists. And is this not, in essence, the primary purpose of government?