South Carolina Law Review

Volume 67
Issue 3 *2016 South Carolina Law Review Symposium*

Article 4

Spring 2016

End to End Encryption, the Wrong End

Amitai Etzioni

Follow this and additional works at: https://scholarcommons.sc.edu/sclr

 Part of the Law Commons

Recommended Citation

Etzioni, Amitai (2016) "End to End Encryption, the Wrong End," *South Carolina Law Review*: Vol. 67 : Iss. 3 , Article 4.
Available at: https://scholarcommons.sc.edu/sclr/vol67/iss3/4

This Article is brought to you by the Law Reviews and Journals at Scholar Commons. It has been accepted for inclusion in South Carolina Law Review by an authorized editor of Scholar Commons. For more information, please contact dillarda@mailbox.sc.edu.

END TO END ENCRYPTION, THE WRONG END

Amitai Etzioni*

I. INTRODUCTION

The following article was written and accepted for publication before recent events, especially concerning Apple's refusal to decode the cell phone of one of

---

*I am indebted to Rory Donnelly for extensive research assistance on this paper and to Stephen Saltzburg for comments on a previous draft. It was written after a stimulating dialogue with Peter Raven-Hansen, though he is not party to its failings.

This article was written and posted on SSRN on May 11, 2015 before the terrorist attacks in San Bernardino took place on December 2, 2015. It hence does not deal with the legal issues that were raised when a court ordered Apple to heed the FBI's request that it enable the FBI to read the messages stored on the cell phone of one of the two terrorists who were shot dead after they killed 14 people. Nothing that followed made me find that I should modify the article. On the contrary. The tragic events seem to confirm what I noted before they took place. Frankly, several of the observations qualify as being outright prescient.

Published by Scholar Commons, 2016

the San Bernardino terrorists. The following lines address these developments. I saw no reason to change the article itself.

The director of the FBI stated that it has gone "dark" since Apple started to provide its customers with end to end encryption that only the sender and receivers can encrypt. Those who do not trust the FBI should note that the current director James Comey, risked being fired in order to prevent the Bush Administration from implementing a surveillance program he considered was in violation of the Constitution.[1] Moreover, these doubters should note also that Apple itself claimed that its new encryption was unbreakable. In short, terrorists, kidnappers, and drug lords—who were greatly hampered by being unable to communicate with others without the NSA, CIA, or FBI capturing their messages—now seemed to have a phone that provided them with a secure line of communication as well as a reliable place to store information about targets, participants, and so on, vastly improving their operational capabilities. In response, the FBI asked Apple to help it decrypt one such phone, the one used by the terrorist who killed 14 people in San Bernardino.[2] Apple refused; the court agreed with the FBI and ordered Apple to comply.[3] Apple refused to abide by the court's order.[4] It is appealing the court's ruling, but meanwhile the information in the terrorist's phone was losing its value as the trails go colder.

True, in March 2016 the FBI reported that it found a way to de-encrypt the Apple phone without Apple's help.[5] However, the pro and con arguments still deserve full attention, because Apple is seeking to close the open window the FBI uncovered and Apple and other high tech companies are producing and selling other encryption devices for all kinds of electronic means of communication as well as storage of data, for instance for cloud storage.

Moreover, Apple's lawyers and public relations machine launched a campaign to convince the public that it should be allowed to continue to sell its phone with the new encryption powers to all comers all over the world. The campaign is using what is known as 'throwing in the kitchen sink'; accordingly

---

1. Alina Selukh, *Lawful Hacking: Should, Or Can, The FBI Learn To Overcome Encryption Itself?*, NPR (April 19, 2016), http://www.npr.org/sections/alltechconsidered/2016/04/19/474842912/lawful-hacking-should-or-can-the-fbi-learn-to-overcome-encryption-itself.

3. Kim Zetter, *Magistrate Orders Apple to Help FBI Hack San Bernardino Shooter's Phone*, WIRED (Feb. 26, 2016), https://www.wired.com/2016/02/magistrate-orders-apple-to-help-fbi-hack-phone-of-san-bernardino-shooter/.

4. Eric Lichtblau and Katie Benner, *Apple Fights Order to Unlock San Bernardino Gunman's iPhone*, NY TIMES (Feb. 17, 2006), http://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html?_r=0.

5. Devlin Barrett and Daisuke Wakabayashi, *FBI Opens San Bernardino Shooter's iPhone; U.S. Drops Demand on Apple*, WALL STREET JOURNAL (Mar. 28, 2016), http://www.wsj.com/articles/fbi-unlocks-terrorists-iphone-without-apples-help-1459202353.

Apple does not rely on one argument or two, but a handful, adding some more every other week, including some very far-fetched ones.

Actually the Constitution is quite clear on the matter at hand. The Fourth Amendment does not state that the government may not "search" phones, homes, papers and persons; it merely bans "unreasonable" searches.[6] Moreover, the Constitution provides a mechanism for determining what searches are reasonable: the courts.[7] In the case of the phone of the dead San Bernardino terrorists, the courts ruled that the search is reasonable.[8] Apple argues that this matter should not be decided by the courts but by Congress.[9] This is obviously a disingenuous proposal because it is very well known that Congress is so polarized it cannot attend to most anything. And if it did, it would take many months. Most obvious, dealing with cases is the job of courts, not Congress.

Apple argues that the FBI is seeking to violate its First amendment rights, because courts recognized codes as a form of speech. However, no right is absolute. Famously, one cannot shout fire in a crowded theater, precisely because such a shout may cost many lives. Apple also argues that the government might be able to prevent some speech but not make Apple say what it refuses to say, which is what is called for if Apple is required to write a code needed to open the terrorist's phone. However the courts allowed such a requirement very often when public safety is involved. For instance, they require warning labels on cigarette packages and content labeling on foods and medications, among many others.

Lawyers argue that the government cannot make Apple work for it, impose costs on it, that such imposition would amount to "taking" (under the Fifth amendment) or even slavery (in violation of the Thirteenth amendment). These arguments have been tested by the courts on several occasions because practically all regulations the government issues—including those involving the protection of children, consumers, employees and the public—exact some costs. Apple surely can afford decode a phone whose code it forged.

Above all, Apple argues that if it decodes this phone everyone's privacy will be endangered.[10] This assumes that it would disclose how it decoded its own phone, rather than subject this code to high power encryption.

High tech corporations and their supporters are concerned that if a key were created, the software would be stolen or leaked. Cook warned that

---

6. U.S. CONST. amend. IV.
7. U.S. Const. art. III, § 1.
8. *See* Zetter, *supra* note 3.
9. *See* Katie Benner, Eric Lichtblau, and Nick Wingfield, *Apple Goes to Court, and F.B.I. Presses Congress to Settle iPhone Privacy Fight*, NY TIMES (Feb. 25, 2016), http://www.nytimes.com/2016/02/26/technology/apple-unlock-iphone-fbi-san-bernardino-brief.html.
10. *See* Lichtblau and Benner, *supra* note 4.

> [i]n the wrong hands, this software—which does not exist today—would have the potential to unlock any iPhone in someone's physical possession . . . The FBI may use different words to describe this tool, but make no mistake: Building a version of iOS that bypasses security in this way would undeniably create a backdoor. And while the government may argue that its use would be limited to this case, there is no way to guarantee such control.[11]

In response, I suggested on March 7, 2016 that Apple (and other high-tech corporations) leave the encryption software as it is—not introduce a vulnerability or a backdoor—but develop a key to unlock phones, a key they would keep. Thus, once a court orders that a given phone must be unlocked, the FBI would bring it to Apple (or Google or whatever other high tech corporation is involved)—and they will unlock the phones they produced, and turn over to the FBI any information that's found—but not the key.[12] (To apply the same idea to phones still in the hands of bad actors requires considerable additional collaboration between the FBI and the high tech corporations, but the same principle could be applied).

Several AI experts commented on this suggestion. Many thought that although Apple has the technical capability to create a key, the real issue would be keeping it secure. Steve Bellovin from Columbia University's department of computer science responded that "a key can be readily available or it can be secure, it can't be both." According to Phillip Schrodt, a senior research scientist, " . . . the problem is not the technology, it is people getting careless about how they use the technology." David Bantz, Chief Information Architect for the University of Alaska system, noted that "NYC and [the] FBI have hundreds of phones they want to unlock. That would entail a process involving many people and loading the OS on many phones. That makes it possible maybe even likely that one of those people entrusted with that power is coerced or bribed or is clumsy enough to put it in the hands of criminals."[13] I was surprised to hear during a meeting on May 11, 2016 at the Council of Foreign Relations (a rare one, on the record) District Attorney Vance informing the audience that until September 2014 his office was able to routinely send phones to Apple; Apple would open them and send back the information within a day or two.[14] The reason Apple stopped, Vance implied, was that in September 2014, it started

---

11. Tim Cook, "A Message to Our Customers," (February 16, 2016) accessed March 29, 2016 at http://www.apple.com/customer-letter/.

12. COMMUNITARIAN OBSERVATIONS, (March 7, 2016) https://communitariannetwork.org/sites/communitariannetwork.org/files/downloads/CommOb_March72016.pdf.

13. COMMUNITARIAN OBSERVATIONS, (March 18, 2016) https://communitariannetwork.org/sites/communitariannetwork.org/files/downloads/CommOb_March182016.pdf.

14. "Privacy and Security in a Digital Age," May 11, 2016, COUNCIL ON FOREIGN RELATIONS http://www.cfr.org/privacy/privacy-security-digital-age/p37845.

advertising that it was the only company that sold phones whose encryption could not be broken.[15] It seems that concerns for profits, a fully legitimate concern, played a key role in Apple's sudden refusal to cooperate with law enforcement and national security authorities.

In response to the repeated claim by high-tech corporations that there is no way such a key can be kept secure, even if it never left their premises and was protected by their own high powered encryption—I note that Coca Cola kept its formula secret for many decades. And that leaks about secrets from the FBI, during the last 25 years, have been very rare. And that if the key was 'leaked,' high tech corporations would modify their encryption software by patching it up, as they often do, and develop new keys. In effect this is what Apple sought to do when it learned that the FBI found a way to unlock Apple's iPhone. Most importantly, I agree with Vance, who argued that one must weigh "the risk of maintaining the ability to open a phone by the company . . . versus . . . the consequence to law enforcement of not being able to access those phones."[16] The answer seems self-evident.

I am sure Apple will come up with more arguments, still. All these arguments should be sorted out. However, at the end of the day it should not be up to CEOs seeking to maximize profits to have the final say in matters concerning high risk to public safety. Apple is not above the law. And its managers should note that when the next major terrorist attack takes place, whether or not it includes a dirty bomb—we are surely to learn that Apple's phones facilitated the attack. This should give pause to Apple's shareholders and customers. It is likely to hurt Apple's bottom line.

II. ULTIMATE ENCRYPTION

Tech companies are increasingly adopting what I call "ultimate encryption" (UE), that is, encryption schemes in which only the sender and the receiver of the communication can decrypt the message. Hence, tech companies are unable to comply when authorities present a search warrant, even if the warrant is fully authorized by a court and based on the government having provided a sufficient level of particularized suspicion. Such a scheme is also provided by tech companies for select forms of storing of information.

Beginning in 2014, Apple and Google moved to encrypt their customers' stored data in this way by default.[17] This is the case for Apple's laptop and desktop computers, for which Apple's Yosemite operating system encrypts the

---

15. *Id.*

16. *Id.*

17. *See* Allison Grande, *Apple, Google To Face Legal Backlash To Encryption Plan*, LAW360 (Sept. 25, 2014, 2:12 PM), http://www.law360.com/articles/580697/apple-google-to-face-legal-backlash-to-encryption-plan.

contents of a computer's hard drive by default,[18] as well as all data stored on the iPhone.[19] UE is provided for communications and transactions, by Facebook-owned messaging service Whatsapp, Apple messaging service iMessage, and Apple video-calling service Facetime.[20] Yahoo and Google are likewise moving to adapt UE encryption for their popular email services.[21] Others are very likely to follow.

As a result, these information databases and flows are extremely private. Indeed, if users forget their passwords, the tech companies are unable to help them regain access to the information. UE makes it much more difficult for the public authorities, such as the NSA and FBI, to obtain this information pursuant to lawful authority. In Apple's own words, "we wouldn't be able to comply with a wiretap order even if we wanted to."[22] According to Apple, while for "iOS devices running iOS versions earlier than iOS 8.0, upon receipt of a valid search warrant issued upon a showing of probable cause, Apple can extract certain categories of active data from passcode locked iOS devices," for newer devices, "Apple will not perform iOS data extractions as data extraction tools are no longer effective. The files to be extracted are protected by an encryption key that is tied to the user's passcode, which Apple does not possess."[23]

Reference to encryption "by default" means that UE is provided in such a form that the users have to take no particular step to benefit from it. UE is built-in, though it can be disabled if users wish for some reason to avoid it. There is considerable evidence from other fields that when systems move from opt-in to

18. Alex Hern, *Apple Defies FBI and Offers Encryption by Default on New Operating System*, THE GUARDIAN (Oct. 17, 2014), http://www.theguardian.com/technology/2014/oct/17/apple-defies-fbi-encryption-mac-osx.

19. Kevin Poulsen, *Apple's IPhone Encryption is a Godsend, Even if Cops Hate It*, WIRED (Oct. 8, 2014, 6:30 PM), http://www.wired.com/2014/10/golden-key/.

20. Nicole Arce, *WhatsApp Encryption Has Just Made It More Difficult for Gov't to Spy on You*, TECH TIMES (Nov. 19, 2014), http://www.techtimes.com/articles/20515/20141119/whatsapp-encryption-has-just-made-it-more-difficult-for-gov-t-to-spy-on-you.htm; LEGAL PROCESS GUIDELINES, APPLE (Apr. 10, 2015), https://www.apple.com/tw/privacy/docs/legal-process-guidelines-emeia.pdf.

21. Tom Lowenthal, *Yahoo's End-to-End Email Promises Greater Protection for Journalists*, PBS (Apr. 9, 2015), http://mediashift.org/idealab/2015/04/yahoos-end-to-email-promises-greater-protection-for-journalists/.

22. https://www.apple.com/privacy/privacy-built-in/. PRIVACY, APPLE https://www.apple.com/privacy/privacy-built-in/ (last visited Feb. 2, 2016).

23. LEGAL PROCESS GUIDELINES, APPLE (Sept. 29, 2015), https://www.apple.com/privacy/docs/legal-process-guidelines-us.pdf.

opt-out, there is a very high degree of increased use.[24] One should expect extremely few, if any, users to opt out of UE.[25]

While the Stored Communications Act requires that companies provide access to law enforcement data that they store,[26] the widespread introduction of UE is possible because companies are not obligated to store the data in the first place: the U.S. does not have mandatory data retention laws, meaning that companies are under no legal obligation to archive their customers' activities for possible law enforcement access.[27] (The European Union had such a law, but it was invalidated by a court in 2014 and has yet to be reintroduced.[28]

Public authorities have expressed alarm about these developments. FBI Director James Comey, for example, has warned that "encryption threatens to lead all of us to a very dark place," as the "recent default encryption settings and encrypted devices and networks," that is, UE, "will have very serious consequences for law enforcement and national security agencies at all levels."[29] Public authorities refer to what I call UE as forcing police and intelligence agencies to "go dark;" be blinded might be an appropriate phrase. In Comey's words, "if the bad guys don't back up their phones routinely, or if they opt out of uploading to the cloud, the data will only be found on the encrypted devices themselves. . . . Sophisticated criminals will come to count on these means of evading detection. It's the equivalent of a closet that can't be opened. A safe that can't be cracked."[30] Likewise, British Prime Minister David Cameron has asked, "Do we want to allow a means of communication between people which even in extremis, with a signed warrant from the home secretary personally, that we

---

24. *See, e.g.*, David McKenzie, "Enhanced Active Choice: Utilizing Behavioral Economics to Increase Program Take-up," World Bank, April 29 2013, accessed May 5 2015 at http://blogs.worldbank.org/impactevaluations/enhanced-active-choice-utilizing-behavioral-economics-increase-program-take-0. *See* Hern, *supra* note 18 (stating that boxes marked "Turn on FileVault disk encryption," and "Allow my iCloud account to unlock my disk" are preselected).

25. *See* David McKenzie, *Enhanced Active Choice: Utilizing Behavioral Economics to Increase Program Take-up*, WORLD BANK (Apr. 29, 2013), http://blogs.worldbank.org/impactevaluations/enhanced-active-choice-utilizing-behavioral-economics-increase-program-take-0.

26. 18 U.S.C. § 2701 (2012).

27. *United States*, ELECTRONIC FRONTIER FOUNDATION (May 5, 2015), https://www.eff.org/issues/mandatory-data-retention/us (last visted June 21, 2016).

28. Francesco Guarascio, *EU Executive Plans No New Data Retention Law*, REUTERS (Mar 12, 2015, 2:28 PM), http://www.reuters.com/article/2015/03/12/us-eu-data-telecommunications-iduskbn0m82co20150312.

29. James Comey, Dir. Fed. Bureau of Investigation, Speech at the Brookings Institution Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? (Oct. 16, 2014).

30. James Comey, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?" (Speech, Brookings Institution Washington, D.C., October 16, 2014) accessed April 24 2015 at http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course. *Id.*

cannot read? . . . My answer to that question is: 'No we must not.'"[31] And US Attorney General Eric Holder has stated that it is "fully possible to permit law enforcement to do its job while still adequately protecting personal privacy."[32] Further, Holder stated, "What concerns me about this is companies marketing something expressly to allow people to place themselves beyond the law."[33] Some computer experts hold that these statements are exaggerated; that UE is merely greatly increasing the costs and time authorities must invest in gaining access rather than being completely shut out.[34] All that follows applies even if these observations are true.

The consequences of the introduction of UE to massive and routine use has been acknowledged by some in the industry.[35] For instance, the then-Senior Legal Director of Human Rights for Yahoo!, Ebele Okobi, recognized that making communications over the internet "immune" to any kind of law enforcement poses serious negative implications, raising the prospect that private companies will be unaccountable to elected governments, and that a total lack of policing of the internet can facilitate abusive behavior and threaten, rather than protect, human rights.[36] Others defend these developments on technical and normative grounds. For example, technology reporter Alex Hern argues that "far from being unacceptable, the ability to have a conversation which the government cannot eavesdrop on is a crucial part of what it means to live in a

---

31. Christopher Hope, *Spies should be able to monitor all online messaging, says David Cameron*, THE TELEGRAPH (Jan. 12 2015), http://www.telegraph.co.uk/technology/internet-security/11340621/Spies-should-be-able-to-monitor-all-online-messaging-says-davidCameron.html.

32. *Id.*

33. Julia Edwards, *U.S. Attorney General Criticizes Apple, Google Data Encryption*, REUTERS (Sept. 30, 2013, 2:02 PM), http://www.reuters.com/article/2014/09/30/us-usa-smartphones-holder-idUSKCN0HP22P20140930.

34. *See* Declan McCullagh & Jennifer Van Grove, *Apple's iMessage Encryption Trips Up Feds' Surveillance*, CNET (Apr. 4, 2013, 4:00 AM), http://www.cnet.com/news/apples-imessage-encryption-trips-up-feds-surveillance/ ("Christopher Soghoian, a senior policy analyst at the American Civil Liberties Union, said . . . 'Apple's service is not designed to be government-proof. It's much more difficult to intercept than a telephone call or a text message' that federal agents are used to . . . ." Apple's privacy policy authorizes the company to divulge customers' information about customers to law enforcement when 'reasonably necessary or appropriate' or to 'comply with the legal process.).

35. *See, e.g.*, Panel Discussion, *Defending an Unowned Internet; Opportunities for Technology, Policy, and Corporations* at Harvard Law School (Feb. 3, 2014, 5:00 PM), http://cyber.law.harvard.edu/events/2014/02/defending_an_unowned_internet (discussing broadly the questions of balancing private and public interests by a government facing an "unowned" internet that cannot be properly policed).

36. "Defending an Unowned Internet Opportunities for Technology, Policy, and Corporations," (Panel Discussion, Harvard University, Cambridge, MA) February 3, 2014, accessed May 5 2015 at http://cyber.law.harvard.edu/events/2014/02/defending_an_unowned_internet. *Id.*

democratic country."[37] And the Electronic Frontier Foundation argues that "privacy comes at a cost."[38]

In the following pages I first outline a communitarian normative position that I suggest one ought to apply in deliberating such matters (Part III).[39] I then suggest specific legal grounds under which Congress or the courts might ban UE. (Part IV).[40] The article closes by examining the arguments of those who favor UE despite the harm it poses to security and public safety, and my response to these arguments. (Part V).[41]

III. UNDERLYING ASSUMPTIONS

A. Liberal Communitarianism

This article draws on a liberal communitarian philosophy, which assumes that we, as a nation, face two fully legitimate normative and legal claims—national security and individual privacy—and that neither can be maximized nor fully reconciled, as there is an inevitable tension between these two claims.[42] It thus follows that some balance must be worked out between the conflicting claims. That is, the liberal communitarian model assumes from the outset that the nation is committed to both individual rights and the advancement of the common good, and that neither should be assumed to a priori trump the other.[43] The liberal communitarian philosophy is dedicated to achieving a balance between individual rights and social responsibilities, which emanates from the need to serve the common good.[44] Liberal communitarians thus take for granted that deliberations about legitimate public policy ought to start with the assumption that privacy must be balanced with concern for national security,

---

37. Alex Hern, *How has David Cameron Caused a Storm Over Encryption?*, THE GUARDIAN (Jan. 15, 2015, 10:26 AM), http://www.theguardian.com/technology/2015/jan/15/david-cameron-encryption-anti-terror-laws (promoting conversational privacy as a foundation of living in a democratic country).

38. Cindy Cohn, *Nine Epic Failures of Regulating Cryptography*, ELECTRONIC FRONTIER FOUNDATION (Sept. 26, 2014), https://www.eff.org/deeplinks/2014/09/nine-epic-failures-regulating-cryptography (quoting Riley v. California 134 S. Ct. 2473, 2493 (2014)).

39. *See infra* Part III.

40. *See infra* Part IV.

41. *See infra* Part V.

42. Simon Dawes, *Interview with Amitai Etzioni: A Communitarian Approach to Press Freedom, Privacy and National Security*, MEDIA THEORY, HISTORY, AND REGULATION (Feb. 2, 2014), https://smdawes.wordpress.com/2014/07/02/interview-with-amitai-etzioni-a-communitarian-approach-to-press-freedom-privacy-and-national-security/ ("Liberal communitarianism starts with the assumption that the public's right to privacy must be balanced with concern for national security . . . rather than from the position that any breach of privacy contravenes an inviolable basic right.").

43. *See id.*

44. *See id.*

rather than from the position that privacy intrusions are ipso facto a violation of a basic right or freedom.

The Fourth Amendment provides an important text for the liberal communitarian philosophy when it states that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[45] By banning only unreasonable searches and seizures, it recognizes that there are reasonable ones—those that serve the common good (or, to use a term more familiar to the legal community, the public interest).[46]

The Fourth Amendment recognizes the right of the people "to be secure against unreasonable searches and seizures," and mandates that "no warrants shall issue, but upon probable cause."[47] Thus, the Amendment recognizes that searches may be conducted when police secure a warrant based on probable cause.[48] At the same time, the amendment bans only "unreasonable searches and seizures," and thus implicitly recognizes a category of "reasonable" searches that may be used to promote public safety even without a warrant based on probable cause.[49] That is, the very text speaks of two sides, and hence, a balance between competing interests. This interpretation has repeatedly been affirmed by the Supreme Court.[50] This contrasts starkly with the First Amendment, which states unequivocally that Congress shall make "no law . . . abridging the freedom of speech."[51]

The Supreme Court has used the "the balancing of competing interests" to determine whether to favor privacy or security,[52] allowing such privacy intrusions as the warrantless entry of police into a private house to pursue a fleeing armed robbery suspect,[53] warrantless drug and alcohol testing of train engineers in the wake of a series of train accidents,[54] and even compulsory DNA sampling of those arrested based on probable cause of serious crimes.[55]

---

45. U.S. CONST. amend. IV.

46. *See generally* Alexander A. Reinhart, *Public Interest(s) and Fourth Amendment Enforcement*, 2010 U. ILL. L. REV. 1461, 1469–73 (2010) (discussing what, exactly, a "reasonable search" is under the Fourth Amendment in a varying contexts with a wide variety of public interests in mind).

47. U.S. CONST. amend. IV.

48. *See id.*

49. *See id.*

50. *See, e.g.*, Michigan v. Summers, 452 U.S. 692, 700 n.12 (1981); United States v. Place, 462 U.S. 696, 703 (1983); Tennessee v. Garner, 471 U.S. 1 (1985); Trupiano v. United States, 334 U.S. 699 (1948).

51. U.S. CONST. amend. I.

52. *Summers*, 452 U.S. at 700, n.12 (White, J., concurring) (citing Dunaway v. New York, 442 U.S. 200, 219 (1979)).

53. Warden v. Hayden, 387 U.S. 294, 298 (1967).

54. Skinner v. Railway Labor Execs.' Ass'n, 489 U.S. 602, 621 (1989).

55. Maryland v. King, 133 S. Ct. 1958, 1980 (2013).

B. Within History

Given that there was no new major attack on the US homeland since 9/11, and following an increase in libertarian sentiment and the Snowden revelations—there has been a considerable shift in public sentiment and that of elected officials against government surveillance. There is growing pressure to reduce security measures, especially those introduced under the USA-PATRIOT Act.[56] However, one should note that (a) ISIS has not been effectively countered so far since rising in late 2013 indeed it is spreading to more countries and even continents. (b) A considerable number of Western fighters have gained combat training and experience while fighting with ISIS and other jihadist groups in Iraq and Syria. Thousands of these fighters can enter the US without even the minimal screening provided by visas because they are US citizens or nationals of countries such as France, Germany, and Britain that participate in the Visa Waiver Program.[57] (c) These foreign fighters need to be monitored, in ways approved by law and the courts, to determine who they call overseas, whether they are building networks with other trained terrorists, and what access they have to weapons and bomb-making materials. Such measures may be impossible, however, if they use easily available UE that requires no technological expertise. (d) The Boston Marathon bombing reminds us that the US is not immune to the kind of attacks that occurred in 2014 in Paris, London, and Copenhagen among other Western cities. Indeed, I suggest that it will only take one more major attack in the US for the public to swing back to demanding

---

56. David Domke et al., *Going Public as Political Strategy: The Bush Administration, an Echoing Press, and Passage of the Patriot Act*, 23 POLITICAL COMM. 291, 292 (Feb. 27, 2007) http://dx.doi.org/10.1080/10584600600808844 (citing Edward Epstein, *House Defies Bush, Votes to Repeal Part of Patriot Act*, SAN FRANCISCO CHRONICLE (June 16, 2005), http://www.sfgate.com/politics/article/House-defies-Bush-votes-to-repeal-part-of-2627813.php; Susan Goering, *Roll Back the Infringement on Civil Liberties; Reviewing the Patriot Act*, BALTIMORE SUN (June 16, 2005), http://articles.baltimoresun.com/2005-06-16/news/0506160085_1_patriot-act-act-permanent-seize-property).

57. For. *See* Peter R. Neumann, *Foreign Fighter Total in Syria/Iraq Now Exceeds 20,000; Surpasses Afghanistan Conflict in the 1980s*, THE INT'L CTR. FOR THE STUDY OF RADICALISATION AND POLITICAL VIOLENCE (Jan. 26, 2015), http://icsr.info/2015/01/foreign-fighter-total-syriairaq-now-exceeds-20000-surpasses-afghanistan-conflict-1980s (providing details on the number of Western fighters and the likelihood they will return to commit terrorist acts); Jamie Crawford and Laura Koran, *U.S. Officials: Foreigners Flock to Fight for ISIS*, CNN (Feb. 11, 2015), http://www.cnn.com/2015/02/10/politics/isis-foreign-fighters-combat/; Daniel Byman and Jeremy Shapiro, *Homeward Bound? Don't Hype the Threat of Returning Jihadists*, FOREIGN AFFAIRS (Nov.–Dec. 2014), http://www.foreignaffairs.com/articles/142025/daniel-byman-and-jeremy-shapiro/homeward-bound; Thomas Hegghammer, *Should I Stay or Should I Go? Explaining Variation in Western Jihadists' Choice between Domestic and Foreign Fighting*, AMERICAN POL. SCI. REV., (Feb. 2013), http://hegghammer.com/_files/Hegghammer_-_Should_I_stay_or_should_I_go.pdf.

more security. It seems a poor time to provide terrorists with the ability to communicate and store information with impunity.

C. The Crux of the Matter

One may grant that the introduction of UE is taking place at a time of somewhat heightened security risks, but still wonder what the implications are for private actors, such as Apple and Google, that are introducing UE. The Constitution guides us in determining whether or not *the government* is acting reasonably, which searches it may carry out legally, and which are banned. The Constitution does not hold that private actors have to enable the government to carry out reasonable searches. However, if we reflect on the challenge at hand in normative terms, this observation suggests that the nation can find itself in a dilemma in which it is heads you win, tails, I lose. That is, searches may either be deemed by the courts as unreasonable and hence banned, or as reasonable—but frustrated by the private sector. In line with the liberal communitarian approach briefly outlined above, one looks for ways to better serve both security and liberty.

IV. POSSIBLE LEGAL GROUNDS FOR BANNING UE

This article next suggests four legal grounds on which the courts or Congress could build if they sought to ban the use of UE. All require some interpretation or extending the appeal or meaning of the law or the Constitution, but these are minor compared to such extrapolations that have often taken place in the past. If one can forge a right to privacy out of the "penumbra" of the Constitution, surely one can similarly forge an obligation of the private sector to comply with warrant requirements in order to keep the public secure.[58]

A. Precedent for Requiring Warrant Compliance

The 1990s, during which computer technology developed rapidly, witnessed a number of major controversies over surveillance and information security, sometimes referred to as the "crypto wars."[59] In 1994, Congress passed the Communications Assistance for Law Enforcement Act (CALEA), which required telecommunications carriers to ensure the government's ability to "intercept . . . all wire and electronic communications" as well as "call-

58. *See* Griswold v. Connecticut, 381 U.S. 479, 483 (1965).

59. Julian Hattem, *'Crypto Wars' Return to Congress*, THE HILL (Oct. 20, 2014), http://thehill.com/policy/cybersecurity/221147-crypto-wars-return-to-congress.

identifying information."[60] The law in effect required "telephone companies to redesign their network architectures to make it easier for law enforcement to wiretap digital telephone calls."[61] This act was expanded in 2005 to include "certain broadband and interconnected voice over Internet Protocol (VoIP) services" such as Skype, as these "can essentially replace conventional telecommunications services currently subject to wiretap rules."[62] The United States Court of Appeals for the D.C. Circuit upheld this order in a 2-1 vote in 2006.[63] (However, subsequent efforts by the government in 2010[64] and in 2013[65] to further broaden CALEA failed.)

Now, all that is needed is to extend the normative and legal concepts that underlie these laws to cover encrypted communication and data storage. In effect, for UE to be outlawed.

B. Inherently Dangerous Product

Another rationale for curbing the introduction of UE by the private sector is that it is "inherently dangerous." In legal terms, this entails an "instrumentality or product that poses a risk of danger stemming from its nature and not from a defect."[66] This term is typically used in product liability referencing to the danger posed by a product to the consumer.[67] In some cases, the conception that some products are inherently dangerous led beyond posing liability on those who

---

60. "SEC. 103. ASSISTANCE CAPABILITY REQUIREMENTS," Ask CALEA, February 11 2011, accessed May 5 2015 at http://askcalea.fbi.gov/calea/103.html. 47 U.S.C. § 1002(a)(1) (2012).

61. *The Communications Assistance for Law Enforcement Act (CALEA) of 1994*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/issues/calea (last visited May 5, 2015).

62. FED. COMMC'N COMM'N, FCC REQUIRES CERTAIN BROADBAND AND VOIP PROVIDERS TO ACCOMMODATE WIRETAPS (Aug. 5, 2005), https://apps.fcc.gov/edocs_public/attachmatch/DOC-260434A1.pdf.

63. *D.C. Circuit Affirms FCC CALEA Broadband Order*, DAVIS WRIGHT TREMAINE: ADVISORIES & BLOGS (June 13, 2006), www.dwt.com/advisories/DC_Circuit_Affirms_FCC_CALEA_Broadband_Order_06_13_2006/. *See also* American Council on Educ. v. Fed. Comm'n Comm'n, 451 F.3d 226, 227 (D.C. Cir. 2006) (denying the petition and upholding the Commission's interpretation in the order as lawful).

64. Charlie Savage, *U.S. Is Working To Ease Wiretaps On the Internet*, N.Y. TIMES (Sept. 27, 2010), http://www.nytimes.com/2010/09/27/us/27wiretap.html?pagewanted=all&_r=0.

65. Charlie Savage, *U.S. Weighs Wide Overhaul of Wiretap Laws,* N.Y. TIMES (May 7, 2013), http://www.nytimes.com/2013/05/08/us/politics.

66. *Inherently Dangerous*, MERRIAM-WEBSTER'S DICTIONARY OF LAW (1996), http://dictionary.findlaw.com/definition/inherently-dangerous.html (last visited February 10, 2016).

67. LEGAL INFO. INST., CORNELL LAW SCH., *Products Liability Law: An Overview*, *in* WEX, https://www.law.cornell.edu/wex/products_liability (last visited June, 21, 2016).

make them to banning such products outright.[68] Plastic guns are an example of a product particularly relevant, because like UE they deal with public safety.

In December 2013, Congress renewed a ban on plastic guns that can evade detection by airport metal detectors.[69] This ban was first introduced under the Reagan Administration in 1988, and was renewed and amended in 2003.[70] It makes it "unlawful for any person to manufacture, import, sell, ship, deliver, possess, transfer, or receive any firearm" that is undetectable by "walk-through metal detector," or any firearm component that, when "subjected to inspection by the types of x-ray machines commonly used at airports, does not generate an image that accurately depicts the shape of the component."[71] Congressional Republicans and even the National Rifle Association (NRA) have not opposed this ban. (On the contrary, the existing ban has been criticized for not covering plastic weapons which include a detachable metal part, even if that part is not required to operate the weapon, and Senate Democrats unsuccessfully pushed for an amendment requiring that plastic weapons include a non-detachable metal part.[72])

In recent years, plastic weapons have become more of a security risk due to advances in 3-D printing technology, which have made possible do-it-yourself manufacturing of increasingly sophisticated plastic weapons, beginning with the single-shot "Liberator" pistol in 2013.[73] Some lawmakers are now calling for a more comprehensive ban on all 3-D printed weapons.[74]

In short, when called for, Congress has acted to protect public safety by banning a product, a move that has been supported by both parties in a period they rarely agree on policy matters or any other.[75] There seems to be no legal or

---

68. *See, e.g.*, David Butler, *Victory: Ban on Dangerous Magnets Approved*, CONSUMERS UNION (Sept. 26, 2014), https://consumersunion.org/2014/09/victory-ban-on-dangerous-magnets-approved.

69. Alan Fram, Associated Press, *Congress Renews Plastic Gun Ban for Decade*, HUFFINGTON POST (Dec. 9, 2013), www.breitbart.com/news/daaj40e801.

70. *The Nation: Reagan Signs Bill Banning Plastic Guns*, LOS ANGELES TIMES (Nov. 11, 1988), http://articles.latimes.com/1988-11-11/news/mn-510_1_plastic-guns; *Fram*, supra note 69.

71. 18 U.S.C. § 922(p)(1) (2012). *See also* WILLIAM J. KROUSE, CONG. RESEARCH SERV., RL32842, GUN CONTROL LEGISLATION 111 (2012).

72. Associated Press, *House Passes Plastic Gun Ban*, POLITICO (Dec. 3, 2013, 5:00 PM), http://www.politico.com/story/2013/12/plastic-gun-firearm-ban-100601.

73. Andy Greenberg, *Meet the 'Liberator': Test-Firing The World's First Fully 3D-Printed Gun*, FORBES (May 5, 2013, 5:30 PM), http://www.forbes.com/sites/andygreenberg/2013/05/05/meet-the-liberator-test-firing-the-worlds-first-fully-3d-printed-gun/#a638ffb511e6.

74. Andy Greenberg, *Bill to Ban Undetectable 3D Printed Guns Is Coming Back*, WIRED (Apr. 6, 2015, 7:00AM), http://www.wired.com/2015/04/bill-ban-undetectable-3-d-printed-guns-coming-back.

75. *See, e.g.*, John Schwartz, *Ban on Microbeads Proves Easy to Pass Through Pipeline,* N.Y. TIMES (Dec. 22, 2015), http://www.nytimes.com/2015/12/23/science/ban-on-microbeads-proves-easy-to-pass-through-pipeline.html (discussing Congress' unanimous ban on the sale of products containing microbeads due to the chemicals they attract once these small plastic bits enter the waterways); Lyndsey Layton & Annys Shin, *Lawmakers Agree to Ban Toxins in Children's*

logical reason UE could not be subject to same kind of ban. (One may argue that other nations might produce UE and provide this service to the public. In other such situations the US used various means to pressure nations not to proceed, and of course if they did, it still banned Americans from using such services, for instance, child pornography.)

Granted, such banning of UE is surely going to face a great amount of opposition on ideological grounds (especially by libertarians and civil libertarians) and on business grounds (in the wake of the Snowden revelations, tech companies held that they must provide their clients extra defense against the US government or lose their business, especially overseas). Hence, it would be much better if the tech companies could be persuaded to voluntarily modify UE so that when faced with a warrant, they could accommodate law enforcement—rather than force them to do by acts of Congress or court rulings.

For a fine precedent for such an approach, one can see the actions of the manufacturers of advanced color printers, a technology that could have made it rather easy to produce counterfeit money. The Secret Service, which is responsible for the "integrity of [US] currency," has noted that "methods used in counterfeiting operations have evolved over the years from the traditional method of offset printing to color copiers and, more recently, to scanners, computers and inkjet printers," which has made it possible "for even unskilled operators to produce high-resolution color reproductions," which has in turn "increased the incidence of the manufacturing and passing of office machine notes."[76]

To deal with this threat, printer manufacturers have cooperated with the government and agreed voluntarily to incorporate anti-counterfeiting measures into their products.[77] This includes yellow dot patterns that allow the US government to determine the serial number of the printer used to print a document, making it easier to track counterfeited notes back to their source.[78]

Items, WASH. POST (July 29, 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/07/28/AR2008072802586.html (noting Congress' agreement to ban certain harmful toxins found in some plastic children's products).

76. "Know Your Money: Advanced Technologies in Counterfeiting," United States Secret Service, 2014, accessed May 5 2015 at http://www.secretservice.gov/money_technologies.shtml.*Know Your Money*, CITY OF WEST FARGO (Oct. 21, 2013), http://www.westfargond.gov/Home/Details.aspx?ID=1053 *(citing* KNOW YOUR MONEY, U.S. SECRET SERVICE, www.secretservice.gov/data/knowyourmoneyapril08.pdf (last visited June 21, 2016)).

77. *See, e.g.*, Jason Tuohey, *Government Uses Color Laser Printer Technology to Track Documents*, PCWORLD, http://www.pcworld.com/article/118664/article.html (last visited May 5, 2015); Jamie Beckett, *HP Helps U.S. Clamp Down on Counterfeiting*, HP (Sept., 2003), http://www.hpl.hp.com/news/2003/july_sept/counterfeit.html.

78. Tuohey, *supra* note 77.

Xerox "pioneered this technology," in the 1980s.[79] Other corporations such as Hewlett-Packard (HP) have been open about their cooperation with the US government to combat counterfeiting, with HP stating that its "imaging and printing business made the effort to integrate anti-counterfeiting measures into [its] devices."[80]

The Electronic Frontier Foundation, which secured a list of participating manufacturers in 2008 through a Freedom of Information Act request and decoded the yellow dot pattern for one device,[81] warns that this "purported effort to identify counterfeiters" means that a "communication tool you're using in everyday life could become a tool for government surveillance."[82] However, a Secret Service spokesperson has stated that this technology is "strictly a countermeasure to prevent illegal activity specific to counterfeiting."[83]

UE deserves the yellow dot treatment: the tech corporations should be able to abide by court orders and law enforcement should use such power only to fight terrorism and major crimes—just as the TSA is allowed to perform administrative searches at airports "'for the purpose of detecting weapons or explosives and not in order to uncover other types of contraband.'"[84]

C. Compelling Public Interest

Still another rationale for banning UE is that the need for the government to gain access to communications relating to terrorism or major crimes is compelling enough to outweigh a suspect's privacy interest. The Supreme Court has carved out a large category of searches that it deemed "reasonable" even in the absence of a search warrant based on individualized suspicion, that of searches justified by "special needs, beyond the normal need for law enforcement."[85] These include routine inspections by personnel from the

79. Jason Tuohey, "Government Uses Color Laser Printer Technology to Track Documents," PCWorld, November 22 2014, Accessed May 5 2015 at http://www.pcworld.com/article/118664/article.html. *Id.*

80. "HP Helps U.S. Clamp Down on Counterfeiting," HP, September 2003, Accessed May 5 2015 at http://www.hpl.hp.com/news/2003/july_sept/counterfeit.html. Beckett, *supra* note 77.

81. Seth Schoen, *Secret Code in Color Printers Lets Government Track You*, ELECTRONIC FRONTIER FOUND. (Oct. 17, 2005), https://www.eff.org/press/archives/2005/10/16.

82. *Printer Dots*, ELECTRONIC FRONTIER FOUND. (Mar. 16, 2011), https://www.eff.org/foia/foia-printer-dots.

83. Mike Musgrove, *Sleuths Crack Tracking Code Discovered in Color Printers*, THE WASHINGTON POST (Oct. 19, 2005), http://www.washingtonpost.com/wp-dyn/content/article/2005/10/18/AR2005101801663.html.

84. United States v. Fofana, 620 F. Supp. 2d 857, 863 (S.D. Ohio 2009) (quoting United States v. Pulido–Baquerizo, 800 F.2d 899, 902 (1986)).

85. New Jersey v. T.L.O, 469 U.S. 325, 351 (1985) (Blackmun, J., concurring).

Occupational Safety and Health Administration;[86] warrantless searches by administrative authorities in public schools, government offices, and prisons;[87] drug testing of public transportation and other government employees;[88] and inspection of automobile junkyards.[89] In all of these cases, the search is considered reasonable because a court found the government's regulatory interest outweighs the individual's privacy interest.[90] The Supreme Court allowed suspicionless, warrantless drug and alcohol testing of train engineers in the wake of a series of train accidents, for example, based on the government's "compelling" interest in ensuring "the safety of the traveling public,"[91] and allowed sobriety checkpoints to catch drunk drivers due to the "magnitude of the drunken driving problem [and] the States' interest in eradicating it."[92]

If such searches are reasonable even in the absence of a search warrant and allow for wide searches of a large number of innocent people, surely the same applies to searchers when the government *does* in fact have a warrant, issued by a court that ruled that there was sufficient individualized suspicion to issue such a warrant. Needless to say, the government has a compelling interest in fighting the terrorism threat, particularly if one accepts that counterterrorism is indeed different from the "normal need for law enforcement."[93] (The same points hold for major crimes such as murder and kidnapping).

D. Obstruction of Justice

Finally, one may justify banning UE on the grounds that it entails obstruction of justice. (This might be a less strong ground than those outlined so far, but it is included in the tradition of throwing everything in, including the kitchen sink.) According to the federal statutes that deal with this concept,[94] obstruction of justice may be summarized as "any act that is intended to interfere with the administration of justice," including "any attempt to hinder the discovery, apprehension, conviction or punishment of anyone who has

---

86. *See, e.g.*, Marshall v. Barlow's, Inc., 436 U.S. 307, 320, n.16 (1978) (stating OSHA searches without consent are still subject to the warrant requirement, but with a lower probable cause standard).

87. *See, e.g.*, *T.L.O.*, 469 U.S. at 341 (stating that teachers do not need probable cause to search students, but the search must be reasonable under the circumstances).

88. *See, e.g.*, Nat'l Treasury Emp. Union v. Von Raab, 489 U.S. 656, 679 (1988) (holding that "suspicionless" testing of government employees applying for promotions is reasonable).

89. *See, e.g.*, New York v. Burger, 482 U.S. 691, 708–09, 711 (1987) (holding that warrantless inspection of junkyard that met certain criteria was reasonable).

90. *See Marshall*, 436 U.S. at 320; *T.L.O.*, 469 U.S. at 341; *Nat'l Treasury*, 489 U.S. at 679; *Burger*, 482 U.S. at 708.

91. Skinner v. Ry. Labor Execs. Ass'n., 489 U.S. 602, 621 (1989).

92. Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 451 (1990).

93. *See* Amtai Etzioni, *A Liberal Communitarian Paradigm for Counterterrorism*, 49 STAN. J. INT'L L. 330, 347–56 (2014).

94. *See, e.g.*, 18 U.S.C. §§ 1501–1521 (2012).

committed a crime."[95] The association of UE with obstruction of justice is suggested by the remarks of Attorney General Holder that tech companies are "thwarting our ability" to "lawfully obtain information in the course of an investigation,"[96] and by FBI Director Comey that "cases could be stalled" and "[j]ustice may be denied, because of a locked phone or an encrypted hard drive."[97]

One may argue that UE does not necessarily expose tech companies themselves to this charge because obstruction of justice only applies when there is a "specific intent to obstruct the proceeding." For federal criminal cases, there is the additional requirement "that a proceeding was actually pending at the time [of the obstruction] and there must be a nexus between the defendant's endeavor to obstruct justice and the proceeding, and the defendant must have knowledge of this nexus."[98] Thus, tech companies that deprive themselves of the ability to access their customers' encrypted data *in advance*—one might say—are not vulnerable to a charge of obstructing justice, as they could be shown to not to have *intent* to obstruct justice.

In response, one notes that the tech companies greatly expanded their encryption schemes in reaction to of the extent of government surveillance, and thus in effect moved to obstruct law enforcement. As we have seen, where UE was once available only to tech-savvy individuals, Apple, Google and others are now making it a default measure in data storage and communications that is now very widely available and requires people to exert themselves only if for some reason they seek to override it.

V. COUNTERARGUMENTS

A. Ask the Sender or Recipient?

Defenders of UE might argue that the government could force suspects to decrypt the information stored in their smart phones or the communications they

95. *What You Should Know about Obstruction of Justice*, OHIO ST. B. ASS'N (Nov. 23, 2014), https://www.ohiobar.org/forpublic/resources/lawyoucanuse/pages/lawyoucanuse-132.aspx.

96. Eric Holder, U.S. Att'y Gen., Remarks by Attorney General at Holder at the Biannual Global Alliance Conference Against Child Sexual Abuse Outline (Sept. 30, 2014) (transcript available at http://www.justice.gov/opa/speech/remarks-attorney-general-holder-biannual-global-alliance-conference-against-child-sexual).

97. James Comey, Dir. of Fed. Bureau of Investigation, Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? (Oct. 16, 2014) http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

98. *Id.*

sent or received.[99] In cases relating to child pornography and mortgage fraud, courts held that the government may force suspects to decrypt stored information. (These rulings were not unequivocal, but rather hinged on the fact that the government already knew "with reasonable particularity"[100] of the "existence and location of subpoenaed documents rulings," that is, the existence of the data was a "foregone conclusion."[101] Thus, the Fifth Amendment privilege against self-incrimination did not apply on the basis that "the Fifth Amendment does not independently proscribe the compelled production of every sort of incriminating evidence."[102] On the other hand, another case upheld a Fifth Amendment defense against forcing a suspect to decrypt their files, on the basis that there was no "foregone conclusion."[103])

However, even if the government may legally compel a suspect to decrypt their files or communications, this approach is vastly inferior from a national security and law enforcement viewpoint, because it prevents the government from gaining information about the suspect's contacts, plans, and preparations—before they are tipped off that the government is on to them.

B. Bad for the Goose, Bad for the Gander?

Defenders of encryption argue that backdoors, key recovery, or other limits on encryption that facilitate the authorities' access to otherwise secure data are themselves "inherently dangerous," as they may also be used by foreign governments or cyber criminals to bypass encryption used by the US government, companies, or private citizens.[104] While this is technically correct,

---

99. *See generally* Dan Terzian, *The Fifth Amendment, Encryption, and the Forgotten State Interest*, 61 UCLA L. REV. DISC. 298 (2014) (analyzing the complex legal issues surrounding decryption of data in criminal investigations).

100. *Boucher*, 2009 WL 424718, at 3 (citing *In re* Grand Jury Subpoena, 1 F.3d 87, 93 (2d Cir. 1993)).

101. In Re Grand Jury Subpoena to Sebastien Boucher. Accessed May 5 2015 at http://volokh.com/posts/1235508933.shtml. *Id.* (citing Fisher v. United States, 425 U.S. 391, 411 (1976)).

102. *Fisher*, 425 U.S. at 408.

103. *See* Orin Kerr, *Eleventh Circuit Finds Fifth Amendment Right Against Self Incrimination Protects Against Being Forced to Decrypt Hard Drive Contents*, THE VOLOKH CONSPIRACY (Feb. 23, 2012, 6:45 PM), http://volokh.com/2012/02/23/eleventh-circuit-finds-fifth-amendment-right-against-self-incrimination-not-to-decrypt-encyrpted-computer/ (quoting decision holding that there was no foregone conclusion whether the files existed in the known location). *See also U.S. v. Doe (In re: Grand Jury Subpoena Duces Tecum dated March 25, 2011)*, ELECTRONIC FRONTIER FOUND. (Feb. 23, 2012), https://www.eff.org/cases/us-v-doe-re-grand-jury-subpoena-duces-tecum-dated-march-25-2011 (summarizing case where Eleventh Circuit ruled that decrypting data is testimonial and protected by the Constitution).

104. *See, e.g.* Sarah Andrews, *Who Holds the Key? – A Comparative Study of US and European Encryption Policies*, J. INFO. L. & TECH., http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_2/andrews/ (explaining that defenders of encryption find backdoors, key recovery, and other limitations are dangerous, expensive, and insecure).

it ignores the vital question of how much any given means to bypass encryption will weaken that encryption, and to what extent this risk to personal security is manageable and acceptable given corresponding benefits to law enforcement and national security.

To fully respond to this challenge, one must study the various measures that are being considered to allow the authorities to discharge their duties without unduly weakening encryption, which is a highly technical subject. Moreover, it is, to a significant extent, subject to future development rather than merely evaluating available measures. Suffice it to say, it seems reasonable to expect tech companies be able to rise to this challenge and develop such measures. And even if cyber criminals found ways to benefits from any limit on encryption introduced for helping the government, such leaks could be patched and others implemented to comply with the government's legitimate needs.

C. Imported Encryption?

American tech companies argue that in a competitive global marketplace, if they do not provide UE to their customers, foreign companies will do so, and they will lose a competitive advantage—and the public will not be more secure. That, due to the open and global nature of the internet, encryption software cannot be kept out of the US or out of the hands of terrorists.[105] If one follows this logic, however, then Apple and Google should market medications used overseas but not approved by FDA, and distill and distribute heroin—foreigners do it . . . Indeed, there are numerous products foreign firms make and provide that the US seeks to keep out of the hands of Americans. One may say that UE software is different because importation of software is much more difficult to bar than regular products. However, the US effectively bars the downloading of child pornography[106] and spyware and adware.[107] The use of malware was first successfully prosecuted in the 1980s under the Computer Fraud and Abuse Act, which has since been updated.[108] Many states also have laws against "computer

---

105. *See, e.g.*, Sabri Ben-Achour, *FBI Head Concerned Over Apple and Google Encryption*, MARKETPLACE (Oct. 17, 2014, 10:00 AM), http://www.marketplace.org/2014/10/17/tech/fbi-head-concerned-over-apple-and-google-encryption (highlighting the global nature of encryption software).

106. *See* Richard Wortley & Stephen Smallbone, *Child Pornography on the Internet*, CENTER FOR PROBLEM-ORIENTED POLICING (2006), http://www.popcenter.org/problems/child_pornography/print/ (noting that between 1996 and 2006, "ISPs have removed some 20,000 pornographic images of children from the web.").

107. *See, e.g.*, Alan F. Blakley, Daniel B. Garrie & Matthew J. Armstrong, *Coddling Spies: Why the Law Doesn't Adequately Address Computer Spyware*, 2005 DUKE L. & TECH. REV. 25 (2005).

108. *See* Timothy B. Lee, *How A Grad Student Trying to Build the First Botnet Brought the Internet to its Knees*, WASH. POST (Nov. 1, 2013), https://www.washingtonpost.com/news/the-switch/wp/2013/11/01/how-a-grad-student-trying-to-build-the-first-botnet-brought-the-internet-to-its-knees/ (outlining Robert Morris's malware in the mid-1980s that was successfully prosecuted

contaminants" such as malware and spyware.[109] In September 2014, the maker of StealthGenie, a smartphone app used mainly by jealous partners to spy on each other's calls and locations, was arrested after being indicted for "charges of conspiracy, sale of a surreptitious interception device and advertising a surreptitious interception device," in violation of the Wiretap Act.[110] If UE is made illegal, most Americans will not use it, and criminals and terrorists will tend to avoid it because they realize that if they do use it—they will call attention to themselves, and be subject to other modes of surveillance. Moreover, if the US curbed the use of UE, one should expect that most if not all other governments would be quite keen, for their own reasons, to follow suit.

D. How Liberty is Lost

The ideological case in favor of UE draws on the numerous changes made in American law and that of numerous other countries following the 9/11 terrorist attack that have been considered excessive, the Snowden revelations, the absence of major terrorist attacks on US mainland for more than a decade, and the rise of general support for libertarian and civil libertarian ideas. These are summed up by the argument that the US is sacrificing liberty to enhance safety.[111]

A common narrative goes as follows: first, the government, in the name of national security or some other such cause, trims some rights, which raises

---

under the Computer Fraud and Abuse Act). *See also* PROSECUTING COMPUTER CRIMES, OFFICE OF LEGAL EDUC. EXEC. OFFICE FOR U.S. ATT'YS at 1–3, http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf (exploring the history of the Computer Fraud and Abuse Act, noting its successive updates).

109. *Computer Crime Statutes*, NAT'L CONF. OF STATE LEGISLATURES (last updated June 12, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws/ct/386c9aa872d5dfecc76db8da95b138afb86535e6982415e57d60075d9c32fea73cefba624c53a72cf7e071d1620f5649cd90198f6ef2fc26feda4628da36cf8f.aspx (providing list of states that have laws against computer contaminants).

110. Craig Timber & Matt Zapotosky, *Maker of StealthGenie, an App Used for Spying, is Indicted in Virginia*, WASH. POST (Sept. 29, 2014), https://www.washingtonpost.com/business/technology/make-of-app-used-for-spying-indicted-in-virginia/2014/09/29/816b45b8-4805-11e4-a046-120a8a855cca_story.html.

111. *See* Sen. Patrick Leahy & Rep. Jim Sensenbrenner, *The Case for NSA Reform*, POLITICO (Oct. 28, 2013, 9:40 PM), http://www.politico.com/story/2013/10/leahy-sensenbrenner-nsa-reform-098953 (introducing a counteraction to the USA PATRIOT act that arguably threatens citizens' liberty); Stephanie Condon, *NSA Abuses Contradict Obama and Congressional Claims of Oversight*, CBS NEWS (Aug. 18, 2013, 5:30 PM), http://www.cbsnews.com/news/nsa-abuses-contradict-obama-and-congressional-claims-of-oversight/ (exploring incidents of NSA surveillance violations); Chris Soghoian, *US Surveillance Law May Poorly Protect New Text Message Services*, ACLU (Jan. 8, 2013, 9:44 AM), https://www.aclu.org/blog/us-surveillance-law-may-poorly-protect-new-text-message-services (explaining that the government can receive access to seemingly private conversations via platforms like text message, Facebook, and SnapChat).

little alarm at the time. Then a few other rights are curtailed. Soon, more rights are lost and, gradually, the whole institutional structure on which liberal democracy rests tumbles. (Statements that the US has already been turned into a police state, that Americans lost their right to privacy and free speech, and so on and on, are so overblown they need no refutation).

However, there are very few instances of nations that lost their liberty because of such incremental erosion of rights. On the contrary, the evidence shows that typically the relationship runs the other way around: when democratic institutions and policies do not provide an adequate response to new challenges–they are undermined.[112] There are many cases in which liberty was lost when governments did not provide basic security to their people. The Afghans welcomed the Taliban when their country was in anarchy following the retreat of the USSR.[113] The Russians welcomed Putin when their country suffered a major crime wave after the collapse of the USSR.[114] The Egyptians welcomed military rule after two years of revolutionary upheaval. Many in Libya, Syria, and Iraq miss the safety of the old regimes.

Following the 9/11 attacks, when the public was most concerned about additional attacks from sleeper terrorist cells on short order, many Americans were willing to support a strong government, including one that would set aside many basic individual rights.[115] 78% of Americans expressed willingness to "give up certain freedoms to gain security."[116]

However, in the subsequent period, as the government did take numerous and varying measures to enhance public safety and no new attacks occurred, the public gradually restored its commitment to the rights-centered regime. As the government vigorously enacted measures to protect the public—the public's support for constitutional democracy was reaffirmed. That is, when the government reacted firmly to a major challenge, support for constitutional democracy was sustained rather than undermined. In short, to protect our rights, the government needs to provide a reasonable level of security.

---

112. AMITAI ETZIONI, HOW PATRIOTIC IS THE PATRIOT ACT?: FREEDOM VERSUS SECURITY IN THE AGE OF TERRORISM 12–14 (Routledge 2004).

113. *Who Are the Taliban?*, BBC (Sept. 29, 2015), http://www.bbc.com/news/world-south-asia-11451718.

114. Seth Mydans, *20 Years After Soviet Fall, Some Look Back Longingly*, NY TIMES (Aug. 18, 2011), http://www.nytimes.com/2011/08/19/world/europe/19russia.html?_r=0.

115. *See generally Which Freedoms Will Americans Trade for Security?*, GALLUP (Jun. 11, 2002), http://www.gallup.com/poll/6196/which-freedoms-will-americans-trade-security.aspx (outlining polls indicating Americans' willingness to set aside personal freedoms in the name of greater security).

116. "Which Freedoms Will Americans Trade for Security?" Gallup, June 11, 2002, Accessed May 5 2015 at http://www.gallup.com/poll/6196/which-freedoms-will-americans-trade-security.aspx. *Id.*

VI. CONCLUSION

Civil libertarians object to the key new security measures that have been introduced in the wake of the 2001 attacks on the US homeland because they are not based on particularized, individualized suspicion recognized by a court. They argue that these measures violate the constitutional requirement that separates legal from illegal searches. When the same libertarians then support moves by private companies that frustrate security measures that do meet this standard, in full, their position seems quite unreasonable.

Putting aside the question on what legal grounds one may ban UE, there is a major normative issue that is the subtext of the preceding deliberations. That is, there is a profound normative position that finds expression in the Fourth Amendment. Namely, that the government be curbed from searching people—unless there is a clear reason for it to proceed (and a mechanism is provided to determine what is reasonable). This amendment is often understood to protect individuals from an abusive, overreaching government, as we have known through much of human history and still see evidenced in many parts of the world—and, some hold, in the US. However, one should not overlook that the same text also fully recognized that the government may have fully legal and fully justified, legitimate reasons to conduct searches. Hence, when private parties develop, introduce, or promote technologies that make it impossible (or "only" very difficult) for the government to carry out searches courts ruled legitimate, these parties frustrate the essence of the Fourth Amendment, even if technically they may not be required by law to cooperate. It is time for the law to catch up with what good judgment indicates: ban ultimate encryption.

*