A HOOVER INSTITUTION ESSAY

ENCRYPTION SUBSTITUTES

ANDREW KEANE WOODS

Aegis Paper Series No. 1705

Introduction

Policy experts have suggested that the rise of encrypted data is not the end of intelligence collection because law enforcement can look to substitutes—other sources of intelligence, such as metadata—that prove to be just as valuable or more valuable than decrypting encrypted data.[1] This paper focuses on the other side of that insight: on the substitutes available for privacy-seekers beyond encryption, such as placing one's data in a jurisdiction that is beyond the reach of law enforcement. This framework puts encryption in context: there are many ways to keep one's data private, just as there are many ways that the government might get access to that data. While encryption is typically treated as a stand-alone computer security issue, it is a piece of a larger debate about government access to personal data.[2]

Law enforcement officials are, in general, agnostic about the method through which they obtain evidence—what matters is obtaining it. Privacy-seekers are similarly agnostic about how they secure their privacy—what matters is having it. This means that policymakers have a wide set of options—not only about *whether* to allow law enforcement to access personal data, but also *how* to do so. This wide set of options is not reflected in the debate over encryption, which is typically framed in all-or-nothing terms. Some privacy advocates take a stance that seems to allow no room for compromise (an argument that can be boiled down to "it's math!"[3]) and some government actors do the same (essentially arguing, "it's terrorism!"[4]). Widening the scope of the policy discussion to include related issues—what I will call "encryption substitutes"—may increase the chances of compromise and may generate better policy.

In this short essay, I make a few simple assumptions that bear mentioning at the outset. First, I assume that governments have good and legitimate reasons for getting access to personal data. These include things like controlling crime, fighting terrorism, and regulating territorial borders. Second, I assume that people have a right to expect privacy in their personal data. Therefore, policymakers should seek to satisfy both law enforcement and privacy concerns without unduly burdening one or the other. Of course, much of the debate over government access to data is about how to respect

both of these assumptions. Different actors will make different trade-offs. My aim in this short essay is merely to show that *regardless* of where one draws this line—whether one is more concerned with ensuring privacy of personal information or ensuring that the government has access to crucial evidence—it would be shortsighted and counterproductive to draw that line with regard to one particular privacy technique and without regard to possible substitutes.

The first part of the paper briefly characterizes the encryption debate two ways: first, as it is typically discussed, in stark, uncompromising terms; and second, as a subset of a broader problem. The second part summarizes several avenues available to law enforcement and intelligence agencies seeking access to data. The third part outlines the alternative avenues available to privacy-seekers. The availability of substitutes is relevant to the regulators but also to the regulated. If the encryption debate is one tool in a game of cat and mouse, the cat has other tools at his disposal to catch the mouse—and the mouse has other tools to evade the cat. The fourth part offers some initial thoughts on implications for the privacy debate.

The Encryption Debate in Context

The debate about backdoors to encryption leaves little room for compromise. One side characterizes the government's demands for exceptional access as "math denialism": exceptional access simply *cannot* be introduced into a cryptographic system without overwhelming risk.[5] The other side insists that it *must* be done and it can happen, if only cryptographers and software engineers try hard enough. Former FBI director James Comey's recent testimony on the matter is a good example—suggesting that Silicon Valley entrepreneurs simply need to apply the same grit and determination to the encryption problem that they apply to creating new software businesses.[6] The terms of this debate are zero-sum: either it is technologically possible to create a system that is safe but also contains a backdoor, as the FBI asserts, or it is not.

Perhaps there is a better way to frame the debate. The government does not actually seek exceptional access to encrypted data per se; indeed, governments did not seek exceptional access until it became relevant to law enforcement operations. What the government is really after is crucial evidence of crimes and national security intelligence. Encryption is just one barrier—among many—to that evidence and intelligence.

Consider two recent high-profile lawsuits: Apple's refusal to comply with an order to create software to unlock an iPhone[7] and Microsoft's refusal to comply with a warrant compelling the production of evidence stored on overseas servers.[8] These are distinct domains as a matter of public policy, public relations, and law. The first is about whether the All Writs Act authorizes a judge to compel Apple to write new software that can be deployed to weaken the security of the company's phones. This is a case about encryption and technological barriers to the state's ability to access personal data. The Microsoft case, on the other hand, is about whether the Stored Communications Act's warrant provisions apply extraterritorially.[9] This is a case about jurisdictional limits on the state's ability to access personal data. At a legal doctrinal level they are different cases, and in the public eye they are different cases.

But they share many similarities. Both cases are about the authority of a US judge to compel an American company to produce data about one of its customers in connection with a criminal investigation into that customer's activity. In both cases, the company objects to giving the government the relevant information, alleging that to do so would harm the privacy of the company's other customers and would gravely harm the company's reputation.[10] Both companies stand in the way of the government's acquisition of information. Indeed, it may be the case that the increasing use of encryption on devices located domestically is driving the Department of Justice to seek information stored abroad, and vice versa.[11] Viewed in this light, the disputes are quite similar and perhaps even interrelated.

Law Enforcement Substitutes

When Comey testified before Congress on July 8, 2015, he emphasized what is known as the "going dark" problem.[12] The problem is that the rise of default-encrypted communication services like WhatsApp and Signal are taking lines of communication that were once in the clear (unencrypted)—phone lines or other communications that could be intercepted by law enforcement—and making them indecipherable to law enforcement.[13] Comey was hardly the first one to make this argument.[14]

But even if some channels of communication have gone dark, other new sources of intelligence are filling the void. Indeed, as Apple's manager of user privacy testified in that company's dispute with the FBI over access to an encrypted phone: "There are

several other ways the government could have potentially obtained any data stored on the subject device."[15] Far from going dark, some suggest that this is in fact the golden age of surveillance.[16] Encryption is a cryptographic tool for ensuring that only authorized users can read and understand data.[17] It can be deployed on hardware—as in an iPhone, to protect data "at rest"—and it can be deployed by services to protect data "in transit." Importantly, users might have one form of cryptographic security but not another: someone might communicate in the clear but store communications locally in encrypted form; others might communicate through an encrypted channel but store their data locally on an unencrypted disk. Finally, quite apart from these different forms of encrypting data are the use and anonymization of metadata which can be used to identify and track a user's online activities. Each of these is a potential avenue for government evidence gathering.

Equipment Interference

Apple's encrypted iPhone is perhaps the quintessential example of how encryption can make a physical drive—where data rests—unreadable to unauthorized users.[18] If the government seeks access to that encrypted data, it has at least two avenues to pursue: (1) it can attempt to defeat the device's encryption directly, or (2) it can attempt to force the device-maker to defeat the device's encryption. Much of the debate in the FBI's recent attempt to get into an iPhone centered around the second of these avenues—specifically, whether the All Writs Act authorized a court to compel Apple to weaken the encryption on the phone.[19] The matter was resolved, and the FBI's request for Apple's assistance withdrawn, when the government found that it could access the phone's data without Apple's assistance. This would seem to suggest that pathway (1) and pathway (2) are substitutes for each other; the government appears agnostic about which pathway it uses to access critical evidence, so long as it can access that evidence. As I discuss later, it may turn out that one pathway is better than another. But for now it is enough to recognize that there was more than one way to access the encrypted data—that two distinct pathways served as suitable alternatives to each other.

This is relevant to a number of ongoing debates. For example, the Senate recently adopted a recommended change to Rule 41 of the Federal Rules of Criminal Procedure, which allows courts to compel device-hacking on a broad scale.[20] In the United Kingdom as well, similar rules have been adopted. The Investigatory Powers Act, a comprehensive bill that reformed the government's ability to access user data,

authorizes "equipment interference," whereby the government can seek a way around a device's cryptographic security.[21] The motivation for these bills is simple: without a way around the disk-level encryption that protects the devices used by criminal suspects for local data storage, law enforcement officials argue, they cannot access critical evidence.

Metadata

Perhaps the most fundamental challenge to the idea that law enforcement is going dark—or that going dark is actually a problem—is the ready availability of an increasingly powerful source of intelligence: metadata. Metadata or non-content data—"outside the envelope" information, such as sender and receiver identification, IP address, basic subscriber information, date, time, and location data—can be surprisingly revealing.[22] This information is often as valuable or more so for law enforcement than content data.[23] Search-and-seizure law—in the form of the Fourth Amendment doctrine, the Omnibus Crime Control and Safe Streets Act, and the Electronic Communications Privacy Act—draws a sharp distinction between content and non-content data, typically providing fewer legal barriers to law enforcement attempts to access metadata.[24] With enough of this non-content data, law enforcement can gather and infer enormously useful information, such as whom a subject was communicating with, about what, where, and when—much of the most important information for conducting criminal investigations.[25] Since this non-content information is not typically encrypted, cries of going dark may ring hollow. Law enforcement has access to an enormous new trove of non-content data in the form of e-mail logs, GPS location data, and more.

Market-Driven Data

Perhaps the best counter to the going dark worries was made in a report by Harvard's Berkman Klein Center for Internet & Society that argues that law enforcement has access—or will soon have access—to ready substitute avenues of intelligence if and when current channels go dark.[26] The report finds that there are structural reasons why many Internet communication channels will never be fully encrypted. For example, while Apple can afford to take a strong pro-encryption stance because it derives most of its revenue from hardware sales, Google and Facebook make their money on advertisements, which often require the ability to scan through user data, a task that is currently not possible if the data is encrypted.[27] Even if Google and Facebook roll out services that are encrypted, such as WhatsApp (a Facebook product), other services will

remain in the clear. The market for technology services is diverse, and this means that even if some services end up encrypted, others will remain unencrypted—typically so that the company offering the service can monetize user data (primarily through advertisements).

Moreover, even if some communication services go dark, the wide adoption of sensors in everyday products—the so-called Internet of Things—will mean that there are many, many sources of data available to law enforcement beyond phone calls and e-mails.[28] Security cameras, thermostats, Internet-connected refrigerators, voice-enabled assistants like Amazon's Echo and Google's Home—these are a few of the many devices that now collect data about their users, data that can be scooped up by law enforcement agents. Two recent examples are illustrative. In December 2016, law enforcement agents requested data from an Amazon Echo device installed in the home where a crime allegedly occurred.[29] In another example, a Connecticut man is being charged with murder in part based on the data taken from his wife's Fitbit fitness device, which suggested he was lying about his activities on the day of the murder.[30]

Privacy Substitutes

Just as law enforcement agents have alternative sources of evidence outside of encrypted channels, users have a number of alternative avenues for securing privacy. Suppose, for example, that the Feinstein-Burr bill passed, requiring American service providers to hold decryption keys so that they could respond to lawful requests for information.[31] How should a rational privacy-seeker respond? Perhaps by storing data in a jurisdiction that does not respond to requests for mutual legal assistance. Or perhaps by switching to one of the hundreds of encrypted communications services not based in the United States and not subject to the same legal requirements.[32] Or perhaps by deploying anonymity tools to evade detection in the first place.[33] The point is that disk encryption is hardly the only tool available for privacy-seekers to prevent the government from accessing their personal information. Other relevant tools include jurisdictional barriers, other technological barriers, and social norms barriers.

Jurisdictional Substitutes

There are a number of jurisdictional barriers to a government's efforts to access data in the context of an otherwise legitimate investigation.

Blocking Statutes Suppose that the French government investigates a murder in Paris. If the suspect uses an American Internet service like Gmail, which claims to store the user's data in the United States, then the French authorities would not be able to access the suspect's e-mail using French legal process. Instead, the French authorities would need to ask the United States for mutual legal assistance. This process takes upward of a year and effectively means that the content is unavailable for law enforcement purposes. This is all the result of the fact that the data resides in America, and the US Electronic Communications Privacy Act functions as a blocking statute, preventing Google from complying with a legitimate French legal process. The presence of a blocking statute is as much a barrier between law enforcement and the evidence it seeks as any technological barrier.

Uncooperative Regimes Alternatively, suppose that there is no blocking statute on the books, so the service provider or data controller is free to share the data. But it is domiciled in a jurisdiction that is nonetheless unwilling to assist another state to prosecute the relevant crime. This could happen because the countries simply do not have a mutual legal assistance treaty (MLAT)—like, for example, Vietnam and the United States. Or it could happen because, although the two countries may routinely cooperate, they do not agree about the legality of the action in question. For example, if France is investigating allegations of hate speech—the kind of speech that would be protected under the more liberal speech standards provided by the First Amendment in the United States—the French government will not receive mutual legal assistance from the US government, despite the MLAT between the two countries. In either event, a user is able to shelter data—and prevent a state from accessing the data, even for legitimate uses—by moving it to an uncooperative regime. Once again, jurisdictional barriers stand in the way of law enforcement's access to evidence, wholly apart from whatever technological tools are in play.

Uncooperative Service Providers It is also possible that service providers themselves could strategically use jurisdictional barriers to avoid complying with lawful law enforcement requests. For example, suppose that Microsoft stores its customer data in the United States. The Department of Justice serves Microsoft with a warrant to compel an e-mail, and Microsoft flips a switch, sending all of its customer data to Ireland. Now, the data is inaccessible under US law because the Stored Communications Act does not apply to that data. America asks Ireland for mutual legal assistance, and when the request comes in, Microsoft flips a switch, sending the data to Brazil. This could go on and on. Indeed, this is one of the government's key concerns in the Microsoft warrant litigation.[34]

Technological Substitutes

Just as there are jurisdictional substitutes to device encryption, there are technological substitutes as well.

Anonymization Tools Perhaps the most useful way to ensure a measure of privacy online is to operate anonymously. Often, law enforcement will need some amount of identifying metadata before it can search or seize a suspect's digital content data, like e-mails and photos. Suppose that the police receive a tip (or intercept a message) that suggests that a criminal is communicating using the e-mail account "johndoe@gmail.com." Without having some way to connect a particular suspect to this account number, it may be difficult for law enforcement to gather enough evidence to ask for a warrant to get access to the account's contents. This is why privacy-seekers use anonymization tools like Tor, which masks their online activities.[35] If hiding the contents of your communications is good, not having anyone know they are yours is even better. If a user cannot be identified, it does not matter what his messages say (or whether the messages are encrypted, either locally or in transit).

Encrypted Services In addition to encrypting their devices, users can also communicate—both send and receive messages and other content—via an encrypted channel. The largest service to offer encrypted communications is WhatsApp, with a user base of more than one billion users.[36] Although the messages may be stored on users' devices in the clear, they are encoded while in transit so that if law enforcement or any other third party managed to see the message—as it passes through the service's servers, through a local fixed or mobile telecommunications service, or through the larger fiber-optic channels that connect the Internet's major nodes—all that they would see is encoded text. This has led to considerable frustration on the part of law enforcement and states have begun to pursue anti-encryption measures directed at data in transit. Brazil recently jailed a Facebook employee after the company refused to comply with a judicial order to decrypt messages on the WhatsApp service—something the company cannot do after the fact.[37] If a law is passed allowing law enforcement to seek to decrypt devices, a user may still be able to communicate in a secure (encrypted) channel. While Apple's recent dispute with the FBI revolved around access to an iPhone's physical drive, that access would be of limited use to law enforcement if the suspect's communications were entirely encrypted in transit.

Implications for Better Policy

What conclusions can we draw from the fact that encryption is neither the only tool available for privacy-seekers nor the only barrier to law enforcement seeking access to digital evidence? I think at least five conclusions follow.

Society will likely prefer one substitute over another

It seems likely that social preferences will be maximized by picking one domain to delimit government access to data over another. Each domain presents a different set of privacy trade-offs and social preferences will be maximized by some domains more than others. Consider the following privacy concerns, which any particular government action might trigger: How widespread is the privacy harm (how many people's privacy interests are at stake)? How total is the privacy harm (how much stuff—and what percentage—gets revealed to the government)? How long (temporally) is the harm (finite or otherwise)? And so on. Reducing jurisdictional barriers to law enforcement access to data may, on balance, be preferable to creating exceptional access to encrypted services. That is, building a backdoor to Gmail's servers may raise more of these concerns than the contemplated US-UK agreement regarding law enforcement access to data. Even among technological domains, one approach to delimiting government access to data may more closely track social preferences than another. For example, allowing the police to lawfully hack into individual suspects' devices is likely less privacy-invasive than forcing providers to create backdoors to their services.

Blocking one domain places pressure on the others

Suppose that the French government is investigating an attack in Paris. The suspect is thought to have used an encrypted device to communicate with his conspirators using an unencrypted American service. The government has two avenues for accessing relevant evidence: decrypt the phone or obtain the suspect's e-mail from the American service. If jurisdictional barriers prevent the French government from obtaining the e-mails from the American service, there will be significant pressure to decrypt the phone. If the e-mails can be obtained in a timely manner by asking the US service for them, the pressure to decrypt the phone may wither.

Some domains create more displacement than others

Suppose that the US government is contemplating two laws. One would prohibit American providers from encrypting users' communications while the other would

allow the government to obtain warrants to hack into suspects' devices. Which of these laws is more easily evaded by criminals? Undoubtedly, it is the former. If encryption services in the United States were to be weakened or eliminated, they would be replaced tomorrow by hundreds of others offered overseas. Lawbreaking behavior could easily be displaced from one service based in the United States to another based overseas. But under the latter regime, there is no obvious displacement. If the government can obtain and execute warrants to hack into devices, it will be harder for criminals to sidestep the law.[38]

Privacy issues may be better negotiated collectively, not serially

There is a substantial scholarly literature that suggests that negotiators are more likely to achieve mutually beneficial agreements by linking issues that allow each party to compromise on an issue of low priority in exchange for an issue of high priority.[39] This suggests that jurisdictional and technological barriers to government access to data ought to be considered together, not separately. Yet this is not the considered view of either civil society—which treats encryption as a third rail—or government actors, who have largely negotiated these issues discretely. Both sets of actors seem to have calculated that they are better off negotiating about encryption, cross-border data access, and lawful hacking in isolation. Presumably, both sides imagine that they can win in each domain. But if the government cares only about getting relevant information—and we've seen that there are several largely interchangeable avenues for obtaining that information—then to grant government access in *none* of these domains will be suboptimal, just as granting government access in *all* of these domains will be suboptimal. The key is picking the right domain—something that can only happen if they're considered side by side.

Courts may be the wrong institutions for resolving these issues

A corollary of the previous point is that court disputes—which turn on individualized facts and specific doctrinal questions—may not be the best place to create, for the first time, socially optimal trade-offs. Courts take cases on the basis of a particular case or controversy and are typically limited in their inquiry by the facts presented by the parties. This naturally leads court cases to be less sweeping and holistic as policymakers. Often that is a welcome quality; incrementalism has many virtues. But to the extent that courts will resolve major questions of encryption policy without considering available substitutes, they may be less desirable institutions than legislative or executive bodies that can craft more comprehensive reform.

Conclusion

If this analysis is right—that encryption has technological and jurisdictional substitutes—then the implications for the privacy debate are potentially significant. Rather than debate encryption as a stand-alone issue, privacy advocates and government officials should consider these substitutes as a whole. Not only does attention to substitutes make it more likely that policymakers will make better choices about both security and privacy, but it also has implications for institutional competence. Whether these substitutes continue to act as such, however, is an open, empirical question, one that will change as the relevant technology and law change.

NOTES

1 "Don't Panic: Making Progress on the 'Going Dark' Debate," Berkman Klein Center for Internet & Society, Harvard University, February 1, 2016, https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

2 Generally, the debate over encryption occurs at a level of abstraction that suggests a lack of sophistication about the technical aspects of encryption, so I hesitate to suggest that the encryption debate ought to be even broader than it already is. But for reasons that I hope will become clear, I think compromise and sensible policy are most likely when we consider encryption in the context of other, similar domains.

3 See, e.g., Rainey Reitman, "An Open Letter to President Obama: This is About Math, Not Politics," *Medium,* March 18, 2016, http://bit.ly/2drhyR9.

4 See "Encryption Tightrope: Balancing Americans' Security and Privacy," *Hearings Before the Senate Judiciary Committee,* December 1, 2015 (testimony of James B. Comey), http://bit.ly/2d3fgeM.

5 Cory Doctorow, "Obama: Cryptographers Who Don't Believe in Magic Ponies Are 'Fetishists,' 'Absolutists,' *BoingBoing,* March 12, 2016, http://boingboing.net/2016/03/12/obama-cryptographers-who-don.html.

6 See Comey, "Encryption Tightrope."

7 Eric Lichtblau and Katie Benner, "Apple Fights Order to Unlock San Bernardino Gunman's iPhone," *New York Times,* February 18, 2016.

8 In re Warrant to Search a Certain E–Mail Account Controlled and Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016).

9 Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as 18 U.S.C. §§ 1367, 2521, 2701–2711, 3117, 3121–3127 (2013)).

10 See Microsoft's Objections to the Magistrate's Order Denying Microsoft's Motion to Vacate in Part a Search Warrant Seeking Customer Information Located Outside the United States, 8, Microsoft Email Search Warrant Case, 15 F. Supp. 3d 466 (S.D.N.Y. 2014) (No. 13-Mag-2814) (arguing, implicitly, that corporate reputation depends on the firm's ability to reject law enforcement demands); Notice of Objections to February 16, 2016 Order Compelling Apple Inc. to Assist Agents in Search, In the Matter of the Search of an Apple IPhone Seized During the Execution of a Search warrant on a Black Lexus IS300, California License Plate 35KGD203, March 22, 2016, CD No. CM 16-10 (SP).

11 Swire and Hemmings have argued, essentially, that increasing use of encryption causes more pressure on the cross-border data request regime. See Peter Swire and Justin D. Hemmings, "Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program," *New York University Annual Survey of American Law* 71, no. 687 (2017), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2728478.

12 James B. Comey, "Going Dark: Encryption, Technology, and the Balances between Public Safety and Privacy," *Joint Statement with Deputy Attorney General Sally Quillian Yates Before the Senate Judiciary Committee,* July 8, 2015, https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy.

13 Ibid.

14 For a long list of articles addressing the "going dark" problem going back many years, see "Going Dark," *Lawfare* (blog), https://www.lawfareblog.com/topic/going-dark.

15 Declaration of Erik Neuenschwander in Support of Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Governments Motion to Compel Search, paragraph 54, In the Matter of the Search of an Apple IPhone Seized During the Execution of a Search warrant on a Black Lexus IS300, California License Plate 35KGD203, March 22, 2016.

16 Peter Swire and Kenesa Ahmad, " 'Going Dark' Versus a 'Golden Age for Surveillance,' " *Center for Democracy and Technology,* November 28, 2011.

17 Electronic Frontier Foundation, "Surveillance Self-Defense: What is Encryption?" https://ssd.eff.org/en/module/what-encryption.

18 Hayley Tsukayama, "The Two Sides of the Apple Debate," *Washington Post,* February 19, 2016, http://wapo.st/2drHHzn.

19 Apple iPhone case.

20 Swati Khandelwal, "Rule 41—FBI Gets Expanded Power to Hack Any Computer in the World," *Hacker News,* November 30, 2016, http://thehackernews.com/2016/11/fbi-rule-41-hacking.html#sthash.GsAGAKsQ.dpuf.

21 Matt Burgess, "What Is the IP Act and How Will It Affect You?" *Wired,* May 8, 2017, www.wired.co.uk/article/ip-bill-law-details-passed; Daniel Severson, "Taking Stock of the Snoopers' Charter: The U.K.'s Investigatory Powers Bill," *Lawfare* (blog), March 14, 2016, https://www.lawfareblog.com/node/10447.

22 See Matthew J. Tokson, "The Content/Envelope Distinction in Internet Law," *William & Mary Law Review* 50, no. 6 (2009): 2124–25.

23 See generally Steven M. Bellovin, Matt Blaze, Susan Landau, and Stephanie K. Pell, "It's Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law," *Harvard Journal of Law & Technology* 30, no.1 (2016) (describing several ways in which the content/non-content distinction is becoming blurred).

24 Ibid., 3–4.

25 Ibid., 73.

26 Berkman Klein, "Don't Panic."

27 Ibid., 10–12.

28 Ibid., 12–15.

29 Alina Selyukh, "As We Leave More Digital Tracks, Amazon Echo Factors in Murder Investigation," *Morning Edition,* National Public Radio, December 28, 2016, www.npr.org/sections/alltechconsidered /2016/12/28/507230487/as-we-leave-more-digital-tracks-amazon-echo-factors-in-murder-investigation. Amazon initially resisted the police order, and the case is still pending. But the point remains: encryption is no technological barrier to law enforcement access to the device's data. Amazon has since given up the data.

30 Amanda Watts, "Cops Use Murdered Woman's Fitbit to Charge Her Husband," *CNN,* April 26, 2017, www .cnn.com/2017/04/25/us/fitbit-womans-death-investigation-trnd/index.html.

31 See "Compliance with Court Orders Act of 2016," https://www.burr.senate.gov/imo/media/doc /BAG16460.pdf.

32 See Bruce Schneier, Kathleen Seidel, and Saranya Vijayakumar, "A Worldwide Survey of Encryption Products," Berkman Center Research Publication No. 2016-2, February 11, 2016, http://papers.ssrn.com /sol3/papers.cfm?abstract_id=2731160.

33 Tor is the most well-known anonymity software. It claims to "prevent . . . people from learning your location or browsing habits." See Tor Project, https://www.torproject.org.

34 See Brief for the United States, 48, In re Warrant to Search a Certain E–Mail Account Controlled and Maintained by Microsoft Corp.

35 See Thorin Klosowski, "What Is Tor and Should I Use It?" *Lifehacker,* February 21, 2014, https://lifehacker .com/what-is-tor-and-should-i-use-it-1527891029.

36 Cade Metz, "Forget Apple vs. the FBI: WhatsApp Just Switched on Encryption for a Billion People," *Wired,* April 5, 2016, http://bit.ly/2drJYut.

37 David Meyer, "Brazil Arrests Senior Facebook Exec over WhatsApp Aid in Drug Case," *Fortune,* March 1, 2016, http://for.tn/216L67V.

38 The Apple vs. FBI dispute seems like good evidence of just that, since the government was able, with the help of a private firm, to get into the device without Apple's help.

39 See John S. Odell and Dustin Tingley, "Negotiating Agreements in International Relations," in *Negotiating Agreements in Politics,* task force report of the American Political Science Association, 2013, 161, summarizing the literature on issue linkage.

Preferred citation for this publication is Andrew Keane Woods, **Encryption Substitutes**, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1705 (July 17, 2017), available at https://lawfareblog.com/encryption-substitutes.

About the Author

ANDREW KEANE WOODS

Andrew Keane Woods is an assistant professor of law at the University of Kentucky College of Law. He writes about law and technology, and his scholarship has been cited in the *Economist,* the *Wall Street Journal,* the *Washington Post,* Bloomberg, and NPR.

Jean Perkins Foundation Working Group on National Security, Technology, and Law

The Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cyber security, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The working group's output, which includes the Aegis Paper Series, is also published on the *Lawfare* blog channel, "Aegis: Security Policy in Depth," in partnership with the Hoover Institution.

Jack Goldsmith and Benjamin Wittes are the cochairs of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution Working Group, visit us online at http://www.hoover.org/research-teams /national-security-technology-law-working-group.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
The Johnson Center
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200