The Risks of “Responsible Encryption”

Riana Pfefferkorn I February 2018

The Center for
Internet and Society

The Risks of "Responsible Encryption"

Riana Pfefferkorn[1]

February 2018

Abstract. Federal law enforcement officials in the United States have recently renewed their periodic demands for legislation to regulate encryption. While they offer few technical specifics, their general proposal—that vendors must retain the ability to decrypt for law enforcement the devices they manufacture or communications their services transmit—presents intractable problems that would-be regulators must not ignore.

Table of Contents

[1] Riana Pfefferkorn is the Cryptography Fellow at Stanford Law School's Center for Internet and Society.

1 Introduction

With the rise over the past few years in both communications and mobile device encryption, authorities claim their ability to investigate crime and terrorism is “going dark.” [1] To address that issue, the U.S. Deputy Attorney General, Rod Rosenstein, has repeatedly called in his recent speeches for a federal law mandating what he calls “responsible encryption”: the provision of a mechanism for exceptional access by law enforcement to plaintext. [2] The Director of the U.S. Federal Bureau of Investigation (FBI), Christopher Wray, likewise has called for a “responsible solution” to the “going dark” issue. [3] Wray and Rosenstein claim that exceptional access is merited due to the growing number of encrypted mobile devices that the FBI could not open despite warrants authorizing access—nearly 7,800 in fiscal year 2017. [2, 3]

To date, these officials have specified few concrete technical requirements for the exceptional-access scheme they contemplate. Based on what can be gleaned from their remarks, however, their “responsible encryption” proposals present serious difficulties. They would undercut computer security and jeopardize U.S. economic interests, and at the same time would not accomplish the goal of guaranteeing investigators’ evidence-gathering capabilities.

2 Federal Law Enforcement Officials’ “Responsible Encryption” Proposals

In recent public speeches and interviews, Deputy Attorney General Rosenstein and FBI Director Wray have called for changes in technology companies’ implementation of encryption in order to ensure exceptional access by law enforcement to the plaintext of otherwise-encrypted data, both at rest and in transit.

In October 2017 remarks at the United States Naval Academy, Rosenstein discussed the impact on law enforcement of encryption implementations in “[m]ass-market products and services” offered by “service providers, device manufacturers, and application developers.” [2] Specifically, he cited messaging apps “employing default end-to-end encryption” and smartphones whose makers cannot extract data from an encrypted device, even with a court order. [2] Wray echoed Rosenstein’s concerns about these particular challenges—encrypted devices and end-to-end encrypted messaging—in a January 2018 speech at the FBI International Conference on Cyber Security. [3]

In contrast to the present state of affairs, Rosenstein called for "responsible encryption": "effective, secure encryption that allows access only with judicial authorization," requiring that "providers retain the capability to make sure evidence of crime can be accessed when appropriate." [2] Wray likewise called for a "responsible solution" that "both provide[s] data security and permit[s] lawful access with a court order." [3]

Though they do not say so overtly, Rosenstein and Wray appear to disagree over the voluntary or compulsory nature of the "responsible encryption solution." Wray did not specify whether he envisions legislation or, instead, an undertaking by the technology sector on its own initiative. That said, his references to getting "the private sector's help" and "working together" suggest the latter (at least for now). [3] Rosenstein, on the other hand, has expressly contemplated a federal legislative solution to the "going dark" issue. [2] Their respective proposals also seem to differ in scope and technical specifications, though these are hard to discern in each case.

2.1 Scope

The unclear scope of each official's "responsible encryption" proposal complicates the task of responding to them. Both Rosenstein's and Wray's remarks focused on the problems that encrypted mobile devices and end-to-end encrypted messaging apps have ostensibly caused law enforcement to date. Yet a comprehensive "solution" on encryption could go beyond those two particular contexts to cover, say, encrypted voice and video calls and data stored in the cloud—even if the need for regulating those other encrypted services has not yet proved urgent enough to merit a mention in these officials' speeches. This paper uses a close reading of their remarks to make assumptions about each proposal's scope.

Rosenstein's remarks focused more on data at rest than data in transit. For devices, he has not said whether his preferred legislation would cover a range of devices (such as laptop and desktop computers or Internet of Things-enabled appliances), or only smartphones, as in some recent state-level bills. [4] His speeches also leave open whether his preferred legislation would include an exceptional-access mandate for data in transit. As some commentators have pointed out, his proposal is most coherent if read to be limited in scope to mobile device encryption and to exclude data in transit. [5, 6] This paper therefore makes the same assumption.

Wray, meanwhile, discussed both encrypted messaging and encrypted devices in his January 2018 speech. He mentioned "design[ing] devices that both provide data security and permit lawful access" and asked for "the ability to access the device once we've obtained a warrant." [3] Like Rosenstein, he did not specify whether his "responsible solution" would go beyond mobile devices. As to data in transit, he used a financial-sector messaging platform as a real-world example of what a "responsible solution" might look like. [3] Similarly, though, he did not specify whether his "solution" would be restricted to only certain categories of data—for example, communications exchanged through messaging apps (*e.g.*, iMessage, Signal, WhatsApp) but not web traffic (*i.e.*, HTTPS). This paper assumes that Wray's "solution" would, like Rosenstein's, encompass encryption of mobile devices, and that it would also cover messaging apps, but not other forms of data in transit.

2.2 Technical Requirements

As with scope, we know little about the technical requirements either official envisions for his preferred "responsible encryption" scheme. Both officials seem to favor a hands-off approach that requires exceptional access but leaves the specifics of fulfilling that goal up to technology companies. Rosenstein declined to specify any "particular" technical mandate, [2] and Wray acknowledged that a "responsible solution" "may vary across business models and technologies." [3] The only technical requirement that both officials clearly want is a key-escrow model for exceptional access, though they differ on the specifics. Rosenstein seems to prefer that the provider store its own keys; Wray appears to prefer third-party key escrow.

In his October 2017 Naval Academy speech, Rosenstein stated that exceptional-access legislation would not prescribe any specific technical mandate; instead, providers would decide how to build their systems to comply with the fundamental exceptional-access requirement. [2] He disclaimed any regulatory mandate for "the use of a particular chip or algorithm," or "any particular key management technique or escrow." [2]

In subsequent speeches later that month, Rosenstein, while largely recycling his Naval Academy remarks on encryption, clarified his position on the key-management issue. In a speech in London, he said, "Providers could retain the capability to make sure evidence of crimes can be accessed when appropriate, without the government holding the keys or requiring every company to use the same means." [7] Similarly, at an event in Detroit, Rosenstein stated he "do[es] not believe that the government should mandate a specific means of ensuring access," while noting that "[t]he government does not need to hold the key." [8] He repeated this position in a November 2017 media interview, stating, "I do not believe the government should hold the key. … I think the providers ought to have the ability to get in, not us." [9] (The idea is not Rosenstein's: federal law enforcement officials previously called for provider-managed keys in a 2010 legislative proposal. [10]) In support of provider-managed keys, Rosenstein cited "the central management of security keys and operating system updates" and "key recovery when a user forgets the password to decrypt a laptop" as existing examples of "responsible encryption" schemes. [2, 7, 8] At a January 2018 event in Washington, D.C., Rosenstein repeated that he is "not calling for the government to possess the keys," but then equivocated as to whether the manufacturer or a third party should hold them, stating, "those details need to be worked out." [11]

Wray has been even more vague about the technical specifications of his "responsible solution." Beyond noting the potential need for variance "across business models and technologies," the closest he got to specifics was in describing a real-world example: the "Symphony" messaging platform used in the banking industry. [3] In 2015, New York state financial regulators reached an agreement with four banks over their use of the platform, which was marketed as offering "guaranteed data deletion." [3] Under that agreement, as Wray noted, Symphony would retain for seven years a copy of all communications sent by the banks through its platform, and the banks would store duplicate copies of their messages' decryption keys with independent custodians. [3] That agreement was with the *banks* about changing their *use* of the platform, not with the *developer* about changing its *design* of the platform, which makes it a somewhat inapt example for illustrating how *developers* should behave "responsibly" when it comes to encryption. [12] Nevertheless, the fact that Wray mentioned those two elements—retention of messages' plaintext and decryption-key escrow—implies that his "responsible solution" would demand those features of messaging-app developers. For mobile devices, however, he offered no details or examples of how manufacturers should implement "the ability to access the device once we've obtained a warrant." [3]

Taken together, this paper interprets Rosenstein's remarks to contemplate "responsible encryption" legislation, covering only mobile devices, that requires the following:

- For encrypted data at rest on mobile devices, vendors must retain the ability to decrypt ("unlock") devices they manufacture.

- A key-management system wherein keys for exceptional access to encrypted data are held by the provider of the device (or possibly by a third-party escrow agent), not by a government agency.

This paper interprets Wray's remarks to contemplate a "responsible solution" (whether legislative or voluntary), covering mobile devices and messaging apps, that includes the following:

- For encrypted data at rest on mobile devices, vendors must retain the ability to decrypt ("unlock") devices they manufacture.
- For data in transit, messaging apps may not offer end-to-end encryption; the app provider or designated third party must retain the ability to decrypt messages for law enforcement.
- Messaging apps may not offer "ephemeral" messaging; the app provider or designated third party must retain the ability to keep copies of messages sent through the app.
- A key-management system wherein keys for exceptional access to encrypted data are held by one or more third-party escrow agents, not by the provider or a government agency.

The remainder of this paper will highlight some drawbacks of the exceptional-access scheme that both Rosenstein and Wray appear to favor, particularly the key-escrow requirement, and then discuss alternatives to an exceptional-access scheme.

3 Some Risks and Limitations of "Responsible Encryption"

In the field of computer security, there is presently no known proposal for a system that could permit exceptional access to encrypted data without also creating unacceptable risks. [6, 13] The same is true of Rosenstein's and Wray's "responsible encryption" proposals.

True, from a law-enforcement standpoint, exceptional access would surely enable authorities in some instances to gather criminal evidence that is presently beyond their reach. Also, cybersecurity commentator Matt Tait, formerly of British intelligence agency GCHQ, has suggested cryptographically-enforced transparency and baked-in jurisdictional limitations to make such proposals less susceptible to misuse. [5] Nevertheless, their proposals suffer from serious problems that Rosenstein and Wray simply do not engage with, or, at worst, even acknowledge to exist.

3.1 Risks of Increased Key Usage and Access

As said, most of Rosenstein's comments concerning key escrow have envisioned the device manufacturer's management of the key to decrypt devices for law enforcement, whereas in Wray's proposal, keys would be escrowed by a third party.

Rosenstein suggests that manufacturers could manage the exceptional-access decryption key the same way they manage the key used to sign software updates. [2, 7, 8] However, that analogy does not hold up. The software update key is used relatively infrequently, by a small number of trusted individuals. Law enforcement's unlocking demands would be far more frequent. [6] The FBI alone supposedly has been unable to unlock around 7,800 encrypted devices in the space of the last fiscal year. [2, 3] State and local law enforcement agencies, plus those in other countries, up the tally further. [14] There are thousands of local police departments in the United States, the largest of which already amass hundreds of locked smartphones in a year. [14, 15] Thus, Tait's proposal to require the vendor to unlock only devices sold in the country in which the demand issued [5] will not ease the burden on vendors when it comes to populous countries with high rates of smartphone ownership.

Wray's proposal fares no better. Third parties, of course, do not sign a vendor's software updates. The custodians in Wray's third-party key-escrow model would be under all the same burdens as the vendor would be in Rosenstein's self-managed escrow model. If the custodian acts as the escrow agent for several vendors, those burdens would be even greater.

The upshot is that, with law enforcement agencies from around the globe sending in requests to the manufacturer or third-party escrow agent at all hours (and expecting prompt turn-around), the decryption key would likely be called into use several times a day, every day. This, in turn, means the holder of the key would have to provide enough staff to comply expeditiously with all those demands.

The exceptional-access decryption key would have to be accessible by far more people than those currently entrusted with a software update signing key. That puts the key at risk, and also makes it harder to detect inappropriate use of the key. Risk exists even with the software update key, but minimizing its use and accessibility helps to mitigate that risk. [6]

Increasing frequency of use and the number of people with access unavoidably means increasing the risk of human error (such as carelessly storing or leaking the key) or malfeasance (such as an employee releasing the key to an unauthorized outside party in response to extortion or bribery). On behalf of a group of applied cryptography and iPhone security experts, the Center for Internet and Society explained these security risks in an *amicus curiae* brief submitted to the court in the "Apple vs. FBI" case in early 2016. [16]

These risks can be mitigated through security measures such as storing the exceptional-access keys in a hardware security module (HSM) to prevent inadvertent disclosure or theft. An HSM keeps keys physically secure, including through tamper-resistance, and performs cryptographic operations on the inputs it receives. [17] Nevertheless, an attacker could still subvert the controls around the key in order to submit encrypted data to the HSM for decryption. [18] This is tantamount to having possession of the key itself, without any need to attack the tamper-resistant HSM directly. One way for an attacker to get an HSM to apply the key to its encrypted data input is to make the attacker's request appear legitimate by subverting the authentication process for exceptional-access demands.

3.2 Authentication of Exceptional-Access Requests at Scale

Rosenstein's comparison to technical measures for keeping a key secure from inadvertent leakage [2] or theft by attackers does not account for attacks on the vendor's or agent's authorization process for handling law enforcement demands. In addition to the risk of malfeasance by the vendor's or escrow agent's employees, an exceptional-access system could also be exploited by malicious outside actors impersonating law enforcement. If attackers can fool the vendor or escrow agent into unlocking a device, there is no need to expend the effort required to steal the secret key; the attacker achieves effectively the same result. Accordingly, a device manufacturer, app maker, or key-escrow agent will need to vet law enforcement requests from all over the world or at least country. This vetting would encompass both (1) confirming the demand is legitimate, not a fake, and (2) scrutinizing even the *bona fide* demands to ensure they comply with all procedural and substantive requirements imposed by applicable law.

The high volume of law enforcement demands to be expected under an exceptional-access mandate contributes to the authentication problem. As explained above, real, legitimate demands alone are likely to be high-volume, even leaving aside fake demands submitted by fraudsters. And there will be ample incentive for attackers to pepper vendors with fake demands, given the low effort required (compare to present-day phishing attacks) and the payoff if successful. Before Apple strengthened its device encryption in 2011, criminals used to commit fraud using personal data stolen from iPhones with "hack-in-a-box" tools. [6] That trove of data would motivate criminals to fake a law enforcement request in order to get past a device's lock, defeating the purpose of vendors' security enhancements.

Adequately and promptly vetting all requests that come in may be feasible for a large company with vast resources such as Apple (and as said, its employees might still make a mistake). However, a small Taiwanese handset company or indie messaging app maker will likely be unable to do so. If an attacker sends a fake unlock request to the vendor pretending to be, say, a Polish law enforcement agent, and the vendor is fooled into unlocking a device for the attacker or giving the attacker the means to unlock it, it could severely compromise user security. In a provider-managed key-escrow scheme like Rosenstein contemplates, the cost and complexity of authenticating a high volume of global law enforcement requests—not just accurately, but fast enough to meet the quick turn-around time needed in urgent investigations or possibly mandated by the applicable key-recovery law—will fall entirely on the vendor. [13, 19] So, too, in Wray's third-party escrow scheme, that cost and complexity would fall on the escrow agent instead of the vendor. The agent likewise might not have resources equal to the task, particularly if, as said, it is the escrow agent for multiple vendors.

3.3 Impact on U.S. Economic Competitiveness

If Rosenstein's or Wray's exceptional-access proposal were to become law, it would harm the U.S. economy in at least two ways.

First, U.S. vendors and app developers would lose business to overseas competitors in both foreign and domestic markets. Enterprises, governments, and individuals in other countries would be understandably wary of devices and messaging channels that are accessible by the U.S. government, particularly if locally-made alternatives exist. [13] Also, even if a foreign customer is not worried about U.S. government access, an exceptional-access mechanism is a vulnerability that weakens a device's or application's security—another reason not to buy a U.S.-made device or install an app from a U.S. company. Domestic consumers and businesses, too, might choose not to "buy American" for the same reasons. An exceptional-access restriction could lead to a black market for noncompliant mobile devices within the United States.

Second, the weakened security of exceptional access-compliant devices would lead to attackers' gaining access to devices containing personal and business data. They might gain that access by fooling the vendor with an ersatz law enforcement request, or by finding and exploiting a vulnerability in the device attributable to the exceptional-access mechanism. The information the attacker obtains from the device could then be sold or otherwise exploited. That is, compromised devices would lead to identity theft, intellectual property misappropriation, industrial espionage, and other economic harms to American individuals and businesses. These are the very harms from which phone manufacturers are presently protecting Americans by strengthening their device encryption in recent years. [6, 13] An exceptional-access mandate would not only hurt U.S. smartphone manufacturers and app makers, it would end up taking an economic toll on other people and industries as well.

3.4 Shortcomings in Effectiveness

An exceptional-access mandate for device and messaging encryption has one central goal: guaranteeing that law enforcement can get into locked smartphones and read the plaintext of messages. However, this goal can be stymied through other means of preventing law enforcement agents from accessing message plaintext or stored data on a device even if they do successfully compel the provider to give them access. That is, Rosenstein's and Wray's proposals would entail significant security and economic downsides as outlined above, but the ostensible upside will not necessarily be great enough to outweigh them.

One factor undermining the utility of device-level exceptional access is the wide availability and use of encrypted chat applications. Unlocking the phone need not provide access to the data. These chat apps (or other kinds of apps) could require an additional password to unlock messages or other locally-stored app data, such as photos and notes. If the user chooses a reasonable password for the app, then unlocking the phone will not do any good. (Granted, that is a big "if," but apps could impose minimum requirements to force users to select strong passwords.) Applications could further require authentication to several remote cloud services before the data will unlock, even after the user's password is entered. If agents cannot compel all of the providers to cooperate, they will not gain access. Plus, other means besides encryption exist for hiding information on a phone. For example, steganographic applications can be used to hide messages or other information within image files, making it very difficult to find the hidden data on the phone even if it is unlocked. Jihadis have already begun to develop their own such app. [20]

In short, an exceptional-access mandate for devices will never be completely effective. Including encrypted messaging apps in the mandate, as in Wray's proposal, would also be unavailing. Strong encryption would still be available to sophisticated bad actors by switching to foreign-made or open-source apps or building their own, [21] or by adding a plug-in for end-to-end encryption on top of a messaging client that does not end-to-end encrypt messages. [22] U.S. law enforcement authorities, including previous FBI Director James Comey, have long admitted this shortcoming in their exceptional-access schemes. They concede that "[t]he sophisticated user could still find a way" and that law enforcement cannot "solve this entire ['going dark'] problem." [23]

Rosenstein, too, concedes that "[n]o solution will be perfect," and that if his proposal were to be implemented, "some sophisticated criminals may migrate" from vendors that comply to those that do not. However, he maintains that even if "only major providers" that are "used by most criminals and terrorists" comply with an exceptional-access mandate, "any progress in preserving access … would still be a major step forward." [2] (Rosenstein was speaking of communications services, not devices, underscoring the lack of clarity in his proposal. [5, 6] Yet it is true for encrypted devices as well as software that noncompliant offerings would remain available despite a U.S. exceptional-access mandate. A terrorist could still buy a noncompliant device outside the U.S. and bring it in. [13])

Rosenstein thus admits that an exceptional-access mandate is an "80% solution," not a 100% solution, and seems to imply that that would be good enough for him. However, if the most commonly-used devices or messaging apps are exceptional access-compliant, then not only will the majority of bad actors—the average, unsophisticated criminals—be using weakened encryption, so will the majority of innocent people. By imposing an exceptional-access mandate, law enforcement officials charged with protecting the public would create a world wherein the shrewdest wrongdoers have *better* security than the innocents they victimize, who, in turn, would by law have *worse* smartphone and communications security than they do now, leaving them even more vulnerable to those same criminals. This would be a net negative for the general public's data security and safety from crime. Yet Rosenstein and Wray are either unaware of, or have chosen to ignore, this unintended consequence of their "responsible" encryption proposals.

3.5 Summary

This section has described just a few of the many shortcomings of a mandatory key-recovery encryption system, which computer-security experts have documented for two decades. [13, 19] Their "widespread and vocal consensus" was noted by U.S. Senator Ron Wyden (D-OR) in a January 2018 letter to Wray sharply criticizing Wray's speech for "parrot[ing] the same debunked arguments espoused by [Wray's] predecessors" (such as Comey). [23, 24] While Wray said he "just do[es]n't buy" that consensus opinion, [3] Rosenstein has acknowledged the experts' objection that an exceptional access-compliant device "'would be less secure than a product that didn't have that ability.'" [9] "And that may be," he said; "that's a legitimate issue that we can debate—how much risk are we willing to take in return for the reward?" [9] However, for any meaningfully informed debate to occur, Wray must acknowledge that the risk exists at all, and Rosenstein must acknowledge the full extent of that risk—to security, economic, and other interests—and the limitations we could expect on the reward.

4 Alternatives for Law Enforcement Access to Digital Evidence

The lack of a mandatory exceptional-access mechanism in encrypted devices and messaging apps deprives law enforcement agents of the guarantee they previously enjoyed that they could access two particular sources of digital evidence: plaintext messages and data stored on a mobile device. Nevertheless, alternative sources of evidence exist that mitigate encryption's "going dark" effect.

4.1 Low-Cost Means of Accessing Stored Data on Devices

The fact that a device is locked will not always preclude law enforcement from accessing the data stored on it. The device owner may have chosen a weak passcode which law enforcement can guess. Or, rather than using a passcode, the owner may have locked the device using a biometric identifier, such as a fingerprint, with which law enforcement may be able to compel the owner to unlock the device. [25] The data on the device (including messages exchanged through it) may be synced to other devices that law enforcement agents can access, even if they cannot unlock the first device. [26] If the user has turned on backups, the device's contents will be backed up to a cloud storage account (such as iCloud), which the provider likely encrypts against unauthorized access while retaining the key. The provider thus could disclose the backed-up data (again, likely including plaintext of messages) to law enforcement upon receipt of the proper legal process. [26] All of these means of access are already available to law enforcement; they do not require passing a new law, breaking the device's encryption, or circumventing it with other sophisticated or expensive measures.

4.2 Metadata and the Internet of Things

In the absence of access to the contents of encrypted communications or an encrypted device, law enforcement will still be able to obtain metadata about the communications or the device's use. While the term "metadata" can encompass many types of information, two common examples illustrate how law enforcement can use metadata to learn detailed information about an individual's activities. One is location information, which discloses the device owner's movements over time. [26, 27] Phone companies keep records of the cell towers a mobile device connects to [28], and many smartphone apps track location as well. Another is communications metadata, which reveals the device owner's web of contacts. To find out whom a device owner communicated with, law enforcement can obtain call and text-message records and email header information from phone companies, messaging app providers (which may keep this metadata even if the messages themselves are end-to-end encrypted), and email service providers. [26, 27]

In addition, more and more of the items we interact with in everyday life are starting to connect to the Internet of Things (IoT). Already, IoT-connected items range from "smart" thermostats, lightbulbs, and home appliances, to personal health and hygiene products, to children's toys, to automobiles. The IoT will open up a wealth of new sources of metadata for law enforcement, which can use them to learn information about individuals beyond what their mobile devices or communications disclose about them. [26, 27]

With the appropriate legal process, these and other kinds of metadata are available to law enforcement from the third-party entities that collect it. Encryption will probably not impact the availability of metadata to law enforcement anytime soon: because it is hard to encrypt, most metadata is currently not encrypted and is likely to remain so. [26, 27] As above, law enforcement can access these sources of digital evidence without undermining encryption.

4.3 Forensics and Government Hacking

Law enforcement may access data on encrypted, locked mobile devices through the use of mobile forensics tools, or by exploiting vulnerabilities in the device or its software, a technique known as "lawful hacking" or "government hacking."

Private-sector digital forensics companies such as Cellebrite make devices that investigators can use, in the field or in a forensics lab, to extract and analyze data from locked devices while maintaining data integrity for later evidentiary use in court. These tools can recover extensive information, including both metadata (such as account information) and the contents of stored documents and communications (such as messages), and even deleted data. [29] That is, by accessing the device, investigators may thereby gain access to messages they could not read "on the wire" due to end-to-end encryption. Along with their federal counterparts, a number of state- and local-level law enforcement agencies have access to mobile device forensics tools and training, directly or through federal partnerships. [30, 31, 32, 33] The success of tools such as Cellebrite's in circumventing device encryption stands as a counterpoint to federal officials' asserted need to require device vendors by law to weaken their own encryption.

In addition to conducting digital forensics of devices in their possession, investigators may use "lawful hacking" techniques to gain access to a target's device, either locally or remotely. "Lawful" or "government hacking" exploits existing vulnerabilities in consumer hardware and software. [34] These vulnerabilities may be "zero-days"—vulnerabilities that are not yet known to the vendor, and thus have not yet been patched [30]—or "n-days": known exploits for which there is no patch or, alternatively, for which a patch exists, but which the targeted system had left unpatched. [35]

Pursuant to executive-branch policy, participating U.S. government agencies may exploit vulnerabilities for law enforcement, military, or intelligence purposes, and have a process for deciding whether to disclose a zero-day to the vendor. [36] The FBI has been engaging in government hacking since at least the turn of the century, [37] and devotes tens of millions of dollars a year to enhancing its forensics and hacking capabilities as part of its initiative to counter the "threat" of "going dark." [38]

The vulnerabilities exploited by government-hacking techniques contrast with exceptional-access mechanisms in that the latter are purposefully built into a device or system by the vendor for law enforcement's use, whereas the former are inadvertent "bugs" in the vendor's product. Some computer security experts find government hacking preferable, from a security and policy standpoint, to exceptional-access mechanisms. [30] They believe that despite the potential shortcomings they identify, exploiting existing vulnerabilities "represents a viable—and significantly better—alternative" to proposals such as Rosenstein's or Wray's, which would "mandat[e] infrastructure insecurity." [30] Given the near-inevitability of bugs in even the most carefully developed and tested product, consumer products are likely to always have vulnerabilities which law enforcement can exploit. [16, 30] Thus, like digital forensics tools, government-hacking techniques draw into question the necessity of mandating exceptional access.

At the same time, like any security choice, government hacking carries its own set of trade-offs. These shortcomings include the facts that government hacking is expensive, it is difficult to carry out effectively, and the exploit has a limited lifetime, since its discovery or disclosure terminates its usability. [39] However, those consequences are not necessarily as fully understood at this point in time as those of mandatory key recovery, whose risks have been studied for over twenty years. [13, 19] The Stanford Center for Internet and Society explored the potential security ramifications of government hacking in a February 2017 event at Stanford Law School. [40] In short, while government hacking is a positive alternative to an exceptional-access scheme to the extent that it does not require intentionally undermining encryption (with all the security consequences that would flow from that mandate), it cannot be said to be an unalloyed good.

4.4 Summary

These "encryption workarounds" all have their own limitations and trade-offs. None of them is guaranteed to work every time, and their cost and (re)usability will vary greatly. [25] Also, none is a perfect replacement for the guaranteed ability to unlock a smartphone or read the plaintext of messages. [27] However, for the reasons explained above, an exceptional-access mandate would not guarantee that access, either, and yet it would harm the data security of countless average, law-abiding people. At this point in time, no regulation can turn back the clock on the ubiquitous availability of strong encryption for devices and communications. [21]

Law enforcement authorities such as Wray and Rosenstein must adapt to this reality and consider how best to make use of encryption workarounds [27], rather than seek to weaken a technology that is indispensable to data security, the economy, and national security. [26]

5 Conclusion

While the details are unclear, Deputy Attorney General Rosenstein's and FBI Director Wray's respective proposals for "responsible solutions" on encryption both appear to call for mandatory key recovery to guarantee law enforcement exceptional access to encrypted data. This kind of exceptional-access scheme presents significant, intractable information security, economic, and public-safety risks. Yet it cannot guarantee that law enforcement will actually be able to obtain plaintext messages or device data in all cases. Law enforcement officials have repeatedly called for such a mandate over the past two decades, but have continually failed to engage meaningfully with those risks. Rosenstein's and Wray's recent speeches on "responsible" encryption are no different. Meanwhile, law enforcement can take advantage of the ongoing proliferation of alternative sources of digital evidence in order to mitigate encryption's supposed "going dark" effect.

It would be unwise for the United States to pass an exceptional-access mandate into law, whether for device or communications encryption. The propriety of such a law is a matter for vigorous public debate, as Rosenstein has suggested. However, if that debate is to be informed and intelligent, it requires that law enforcement officials be forthright with smartphone vendors, app makers, legislators, and the general public about the technical details of their proposed exceptional-access scheme, the trade-offs it would entail, and the effectiveness of available alternatives for digital evidence-gathering in an age of ubiquitous encryption.

Acknowledgements

Thank you to Professor Dan Boneh of the Stanford University Computer Science Department for his helpful comments on this paper. Riana Pfefferkorn's work is supported by the Stanford Cyber Initiative. Stanford CIS funders are listed at https://cyberlaw.stanford.edu/about-us.

References

[1] Federal Bureau of Investigation, "Going Dark," 2016. https://www.fbi.gov/services/operational-technology/going-dark. Accessed: Nov. 13, 2017.

[2] Office of Public Affairs, Federal Bureau of Investigation, "Deputy Attorney General Rod J. Rosenstein Delivers Remarks on Encryption at the United States Naval Academy," Oct. 10, 2017. https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-encryption-united-states-naval.

[3] Christopher Wray, "Raising Our Game: Cyber Security in an Age of Digital Transformation," Jan. 9, 2018. https://www.fbi.gov/news/speeches/raising-our-game-cyber-security-in-an-age-of-digital-transformation.

[4] Bills introduced in recent years in New York, California, and Louisiana would have required manufacturers of "smartphones" (as defined in the respective texts) to retain the ability to decrypt devices for law enforcement (or, in the California bill, imposed penalties for inability to decrypt), but did not encompass other categories of electronic device. A.B. A8093, 2016 Leg. Sess. (N.Y. 2015); A.B. 1681, 2016 Reg. Sess. (Cal. 2016); H.B. 1040, 2016 Reg. Sess. (La. 2016).

[5] Matt Tait, "Decrypting the Going Dark Debate," *Lawfare*, Oct. 17, 2017. https://lawfareblog.com/decrypting-going-dark-debate.

[6] Susan Landau, "Punching the Wrong Bag: The Deputy AG Enters the Crypto Wars," *Lawfare*, Oct. 27, 2017. https://lawfareblog.com/punching-wrong-bag-deputy-ag-enters-crypto-wars.

[7] Office of Public Affairs, Federal Bureau of Investigation, "Deputy Attorney General Rod J. Rosenstein Delivers Remarks at the Global Cyber Security Summit," Oct. 13, 2017. https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-global-cyber-security-summit.

[8] Office of Public Affairs, Federal Bureau of Investigation, "Deputy Attorney General Rosenstein Delivers Remarks at the 2017 North American International Cyber Summit," Oct. 30, 2017. https://www.justice.gov/opa/speech/deputy-attorney-general-rosenstein-delivers-remarks-2017-north-american-international.

[9] Eric Geller, "POLITICO Pro Q&A: Deputy Attorney General Rod Rosenstein," *POLITICO Pro*, Nov. 9, 2017. https://www.politicopro.com/cybersecurity/article/2017/11/politico-pro-q-a-deputy-attorney-general-rod-rosenstein-164743.

[10] Charlie Savage, "U.S. Tries to Make It Easier to Wiretap the Internet," *N.Y. Times*, Sept. 27, 2010. http://www.nytimes.com/2010/09/27/us/27wiretap.html.

[11] Internet Society, "Fireside Chat with Deputy Attorney General Rod Rosenstein and Kim Hart," Jan. 29, 2018. [Online video]. https://livestream.com/internetsociety/sotn18/videos/169482941.

[12] New York State Department of Financial Services, "NYDFS Reaches Agreements with 4 Major Banks on New Symphony Chat & Messaging Platform," Sept. 14, 2015. http://www.dfs.ny.gov/banking/agree_symphony_09142015.htm.

[13] H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, W. W. Diffie, J. Gilmore, M. Green, S. Landau, P. G. Neumann, R. L. Rivest, J. I. Schiller, B. Schneier, M. A. Specter, and D. J. Weitzner. Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications. *Journal of Cybersecurity*, vol. 1, no. 1, pp. 69–79, November 2015. https://academic.oup.com/cybersecurity/article/1/1/69/2367066.

[14] For example, the Manhattan District Attorney's office has recovered (with warrants) 3,882 locked, encrypted smartphones over the past three years. Office of the Manhattan District Attorney, *Third Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety*. New York, NY: Office of the Manhattan District Attorney, November 2017, p. 5. http://manhattanda.org/sites/default/files/2017%20Report%20of%20the%20Manhattan%20District%20Attorney%27s%20Office%20on%20Smartphone%20Encryption_0.pdf.

[15] U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, *Census of State and Local Law Enforcement Agencies, 2008*. Washington, DC: Bureau of Justice Statistics, July 2011, p. 2. https://www.bjs.gov/content/pub/pdf/csllea08.pdf.

[16] Brief of *Amici Curiae* iPhone Security and Applied Cryptography Experts in Support of Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Government's Motion to Compel Assistance, *In re Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203*, No. 16-cm-10 (C.D. Cal. filed Feb. 19, 2016), docket no. 82.

[17] Jim Attridge, "An overview of hardware security modules." North Bethesda, MD: SANS Institute, Jan. 14, 2002. https://www.sans.org/reading-room/whitepapers/vpns/overview-hardware-security-modules-757.

[18] Mark Gamache. "Why we use hardware security modules." Mark R. Gamache's Random Blog, May 24, 2011. https://markgamache.blogspot.com/2011/05/why-we-use-hardware-security-modules.html.

[19] H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, P. G. Neumann, R. L. Rivest, J. I. Schiller, and B. Schneier. The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption. *World Wide Web Journal*, vol. 2, no. 3, pp. 241–257, 1997. https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/key-study-report.html.

[20] Joseph Cox, "This Custom-Made Jihadi Encryption App Hides Messages in Images," *Motherboard*, Jan. 26, 2018. https://motherboard.vice.com/en_us/article/ne4x7w/muslim-crypt-jihadi-encryption-app.

[21] Ross Schulman, Kevin Bankston, and Jake Laperruque. "The crypto cat is out of the bag." Washington, DC: New America Open Technology Institute, Dec. 8, 2015. https://static.newamerica.org/attachments/12155-the-crypto-cat-is-out-of-the-bag/Crypto_Cat_Jan.0bea192f15424c9fa4859f78f1ad6b12.pdf.

[22] Electronic Frontier Foundation, "How to: Use Tor Messenger (beta) for MacOS," Sept. 8, 2017. https://ssd.eff.org/en/module/how-use-tor-messenger-beta-macos.

[23] Dan Froomkin and Jenna McLaughlin, "Comey Calls on Tech Companies Offering End-to-End Encryption to Reconsider 'Their Business Model,'" *The Intercept*, Dec. 9, 2015. https://theintercept.com/2015/12/09/comey-calls-on-tech-companies-offering-end-to-end-encryption-to-reconsider-their-business-model/.

[24] Ron Wyden. Untitled letter to Christopher A. Wray, Jan. 25, 2018. https://www.wyden.senate.gov/download/?id=B31DD6FF-98E8-490C-B491-7DE6C7559C71&download=1.

[25] Orin S. Kerr and Bruce Schneier. Encryption Workarounds. *Georgetown Law Journal*, vol. __, no. __, pp. __, forthcoming 2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2938033 (Mar. 20, 2017 draft).

[26] Urs Gasser, Nancy Gertner, Jack Goldsmith, Susan Landau, Joseph Nye, David R. O'Brien, Matthew G. Olsen, Daphna Renan, Julian Sanchez, Bruce Schneier, Larry Schwartztol, Jonathan Zittrain, "Don't panic: making progress on the 'going dark' debate." Cambridge, MA: Berkman Klein Center for Internet & Society, 2016. https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

[27] Stephanie K. Pell. You Can't Always Get What You Want: How Will Law Enforcement Get What It Needs in a Post-CALEA, Cybersecurity-Centric Encryption Era? *North Carolina Journal of Law & Technology*, vol. 17, no. 4, pp. 599–643, May 2016. http://ncjolt.org/wp-content/uploads/2016/05/Pell_Final.pdf.

[28] Stephanie K. Pell and Christopher Soghoian. Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact. *Berkeley Technology Law Journal*, vol. 27, no. 1, pp. 117–96, March 1, 2012. http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1928&context=btlj.

[29] Cellebrite, "UFED Ultimate / PA," cellebrite.com, 2017. https://www.cellebrite.com/en/products/ufed-ultimate/. Accessed: Dec. 4, 2017.

[30] George Joseph, "Cellphone Spy Tools Have Flooded Local Police Departments," *Citylab*, Feb. 8, 2017. http://www.citylab.com/crime/2017/02/cellphone-spy-tools-have-flooded-local-police-departments/512543/.

[31] Curtis Waltman, "How the Denver Police Crack and Search Cell Phones," *Vice: Motherboard*, Apr. 11, 2017. https://motherboard.vice.com/en_us/article/how-the-denver-police-crack-and-search-cell-phones.

[32] U.S. Department of Justice, National Domestic Communications Assistance Center, "Executive Advisory Board Meeting Minutes, Appendix D: Program Update," May 17, 2017, pp. 8–17. https://www.documentcloud.org/documents/4178493-may2017eabmeetingminutesappendices.html.

[33] Regional Computer Forensics Laboratory, "About RCFL," rcfl.gov, 2014. https://www.rcfl.gov/about. Accessed: Dec. 4, 2017.

[34] Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau. Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet. *Northwestern Journal of Technology and Intellectual Property*, vol. 12, no. 1, pp. 1–64, April 2014. https://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1/.

[35] Lillian Ablon and Andy Bogart. "Zero days, thousands of nights: the life and times of zero-day vulnerabilities and their exploits." Santa Monica, CA: The RAND Corporation, 2017. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1751/RAND_RR1751.pdf.

[36] The White House. *Vulnerabilities Equities Policy and Process for the United States Government*. Washington, DC: the White House, Nov. 15, 2017. https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.

[37] Kim Zetter, "Everything We Know About How the FBI Hacks People," *Wired*, May 5, 2016. https://www.wired.com/2016/05/history-fbis-hacking/.

[38] Federal Bureau of Investigation. *FY 2018 Authorization and Budget Request to Congress*. Washington, DC: Federal Bureau of Investigation, May 2017, pp. 1-1, 1-15, 5-3. https://www.justice.gov/file/968931/download.

[39] Lawfare, "The Lawfare Podcast: Susan Landau is Listening in on You," *Lawfare*, Nov. 7, 2017. https://www.lawfareblog.com/lawfare-podcast-susan-landau-listening-you.

[40] Stanford Center for Internet and Society, "Government Hacking: Assessing and Mitigating the Security Risk," Feb. 2, 2017. [Online video]. https://cyberlaw.stanford.edu/events/government-hacking-assessing-and-mitigating-security-risk.

About the Author

Riana Pfefferkorn is the Cryptography Fellow at the Stanford Center for Internet and Society. Her work, made possible through funding from the Stanford Cyber Initiative, focuses on investigating and analyzing the U.S. government's policy and practices for forcing decryption and/or influencing the encryption-related design of online platforms and services, devices, and products, both via technical means and through the courts and legislatures. Riana also researches the benefits and detriments of strong encryption on free expression, political engagement, economic development, and other public interests. Prior to joining Stanford, Riana was an associate in the Internet Strategy & Litigation group at the law firm of Wilson Sonsini Goodrich & Rosati, and the law clerk to the Honorable Bruce J. McGiverin of the U.S. District Court for the District of Puerto Rico. She is a graduate of the University of Washington School of Law and Whitman College.

About the Center for Internet and Society

The Center for Internet and Society (CIS) is a public interest technology law and policy program at Stanford Law School and a part of Law, Science and Technology Program at Stanford Law School. CIS brings together scholars, academics, legislators, students, programmers, security researchers, and scientists to study the interaction of new technologies and the law and to examine how the synergy between the two can either promote or harm public goods like free speech, innovation, privacy, public commons, diversity, and scientific inquiry. CIS strives to improve both technology and law, encouraging decision makers to design both as a means to further democratic values. CIS provides law students and the general public with educational resources and analyses of policy issues arising at the intersection of law, technology and the public interest. CIS also sponsors a range of public events including a speakers series, conferences and workshops. CIS was founded by Lawrence Lessig in 2000.