tech:nyc

GOVERNMENT ACCESS TO ENCRYPTED DATA

A Look Ahead to 2017 and Beyond
White Paper ::: Last Update: 4.13.2017

Table of Contents

INTRODUCTION

Ever since Edward Snowden revealed in 2013 that the U.S. government was secretly spying on people around the world, including its own citizens, technology companies have been responding to consumer concerns by making their products more secure. One year after the Snowden revelations, Apple announced iOS 8, the first version of iOS where Apple has no way to decrypt the information on iPhones and iPads.[1] Others companies, including Google, announced similar changes to their platforms not long after. Today, iOS and Android devices running the current or reasonably recent OS are encrypted so that the device and OS makers are not able to decrypt the data on the device.[2]

New York was the first state to react to these technological developments by proposing legislation mid-2015 that would require device manufacturers like Apple and Google to decrypt device storage in response to law enforcement requests. More on this below.

Then, in the first half of 2016, the FBI asked a federal court in California to require that tech companies weaken device encryption and implement cryptographic backdoors into products. And state and federal legislators were debating bills that would take the unprecedented step of requiring cryptographic backdoors. Although the FBI didn't specify how Apple should comply, as explained below, any crippled operating system could be exploited by bad actors to gain unauthorized access to devices running that modified OS. For the first time since the failed Clipper Chip proposal in 1997, consumers were faced with the real possibility that the government would weaken the security of their electronic devices, putting them at greater risk of hacking and unauthorized government surveillance. Ultimately, because it found other means to access a terrorist's iPhone 5c, the FBI dropped its case against Apple. And proposed legislation in Congress, New York, and California appears to have lost momentum and support in the face of strong opposition from cryptographers, digital libertarians, and some members of Congress.

In this white paper, we start by exploring the events of 2015 and 2016, including the 2015 San Bernardino attacks and the FBI's attempt to force Apple, by court order, to create software that would allow the FBI to access the data on an iPhone. Then we summarize arguments made by the world's foremost cryptographers against any legal regime requiring technology companies to unlock devices for the government, including the far-reaching and unintended consequences of

[1] The two subsequent versions of iOS—iOS 9 and 10—are similarly impervious to anyone but the owner, including Apple. As of February 20, 2017, 79% of iOS devices were running iOS 10, and 16% were running iOS 9. Apple typically experiences high update rates upon releasing a new version of the OS.

[2] According to Gartner, 99.6% of new smartphones run either Android or iOS.

substantially weakened device storage technology. We end by examining recent legislative efforts around smartphone encryption and statements made by government officials that suggest potential policy direction as we head into the second quarter of 2017 (including the 2015 report by New York City DA Cy Vance advocating for government device backdoors).

Note: This white paper focuses primarily on the encryption of data "at rest," since that appears to be the focus of recent legislative efforts. However, the concepts and policy arguments do translate to government access to data *in transit* as well. For more on how encryption works, the Washington Post has published an excellent overview of encryption technology.

APPLE VS. THE FBI, 2016

On December 2, 2015, Syed Farook and his wife killed 14 people in a shooting spree in San Bernardino, California. As part of its investigation the FBI sought access to Farook's iPhone 5c, which was running iOS 9, the second version of Apple's mobile operating system to encrypt all data in a way that even Apple couldn't decrypt. (iOS 8, released in September 2014, was the first version to do this.) Before consulting with Apple, the FBI changed the iCloud password associated with one of Farook's accounts, which prevented the automated backup of data to Apple's cloud storage service. Had the FBI allowed Farook's iPhone to back up to iCloud, Apple could likely have provided the FBI with the data they were seeking, as it does in response to other law enforcement requests.

In February 2016, the DOJ filed an order with a magistrate judge in Los Angeles asking the Court to compel Apple to assist the FBI in unlocking Farook's iPhone. The DOJ argued that Apple's participation was necessary to access the phone, relying heavily on a novel reading of the the **All Writs Act of 1789**, an obscure, centuries-old federal law rarely cited as legal authority until 2008, when the federal government and various state governments sought to revive it as legal crowbar for gaining access to cell phones in the absence of any applicable statutes.[3]

It's worth pausing here to underscore how novel and far-reaching the FBI's request was. In February and March of 2016 it received sustained coverage in the national news cycle and captured the interest of a broad swath of the populace, beyond technology insiders and tech policy wonks.[4] Although much of his attention was due to the case's nexus with a terrorist attack, there also seemed to be a growing interest in the limits on government access to private device data.[5]

[3] The Wikipedia entry for the All Writs Act has a useful United States map showing where the US government has attempted to use the Act against Apple and Google.
[4] NPR has a good collection of its coverage.
[5] See, e.g., NBC's coverage; USA Today's coverage; and the New York Times' collection of coverage.

The Act gives judges wide latitude to compel parties to cooperate in cases before them. But the court must consider three factors: (1) the judge must have no other legal options available; (2) the target of the writ (Apple) must be closely connected to the case; and (3) the court order cannot impose an undue burden. The All Writs Act was originally intended to enable federal courts to fill in gaps in the law. But, according to an influential 9th Circuit decision from 1979,[6] it cannot impose new duties on parties that Congress has failed to impose.

On February 16, the Court granted the FBI's request, requiring Apple to provide "reasonable technical assistance" so that the FBI could: (1) bypass the auto-erase function; (2) submit passcodes to the phone via the physical device port, BlueTooth, or WiFi; and (3) ensure that the phone did not introduce its standard password attempt delays.[7] Although the Court gave Apple opportunity to propose alternative technical solutions, it did order Apple to create custom software to achieve these ends.

Apple immediately refused to comply with the request, estimating that the design, creation, validation, and deployment of the required software would necessitate six to 10 Apple engineers dedicating a "substantial portion of their time"— two–four weeks—to create the software.[8]

However, the Court never considered Apple's arguments because the government dismissed the request one day before the hearing was scheduled. Apparently the FBI had found other means to get access to the data on Farook's iPhone, although the FBI never disclosed any details about how it was able to gain access. The FBI has also never revealed whether the information it was able to access was valuable to its investigation.

Apple's Arguments

- Apple already complies with valid subpoenas and search warrants. In the San Bernadino case they made Apple engineers available to advise the FBI and provided data from Farook's iCloud account.
- The Court order violates the All Writs Act, First Amendment, Fifth Amendment (Due Process). More on this below.

[6] *Plum Creek Lumber Co. v. Hutton*, 608 F.2d 1283.

[7] Apple uses a "large iteration count" to slow attempts to access an iPhone, ensuring that it would take years to try all combinations of a six- character alphanumeric passcode. In addition, Apple imposes escalating time delays after the entry of each invalid passcode. Finally, Apple also includes a setting that—if activated—automatically deletes encrypted data after ten consecutive incorrect attempts to enter the passcode.

[8] Apple's motion to vacate, p. 24.

All Writs Act

- There is no precedent for a court ordering a company to weaken the security of its products or services, especially when the company is not directly involved in the case, under the All Writs Act or otherwise.
- The Act does not grant courts "free-wheeling authority to change the substantive law, resolve policy disputes, or exercise new powers that Congress has not afforded them."[9] In short, as the 9th Circuit has held, courts cannot impose a duty on a private party that Congress has failed to impose.[10] This would violate the separation-of-powers doctrine.
- The government never demonstrated that Apple's assistance was necessary to effectuate the warrant.

CALEA

- It's an end-run around the legislative process. If Congress wanted to authorize this, they would have done so, for example, by amending the Communications Assistance for Law Enforcement Act (CALEA).
  - CALEA says that it "does not authorize any law enforcement agency or officer to (1) require any specific design of equipment, facilities, services, features, or system configurations . . . by any manufacturer of telecommunications equipment, or any provider or telecommunications support services; or (2) prohibit the adoption of any equipment . . . or feature."[11] (arguing that Apple qualifies as a provider of "electronic communications services")
  - Instead, efforts to amend CALEA were abandoned in 2013.

First Amendment / Compelled Speech

- Forced creation of code would amount to compelled speech and viewpoint discrimination, which are First Amendment violations.[12] The First Amendment prohibits the government from compelling companies to create code.[13]
- Terrorist organizations are known to use apps that apply their own encryption to the data on the phone. Because that's likely the case here, compelling such speech would not be

[9] *Id* at 25. "Congress has never authorized judges to compel innocent third parties to provide decryption services to the FBI." Apple's motion to vacate, pp. 25–26.

[10] *Plum Creek Lumber Co. v. Hutton*, 608 F.2d 1283, 1290.

[11] 47 U.S.C. § 1002(b)(1).

[12] As a content-based restriction on speech, compelled speech is subject to strict scrutiny.

[13] Citing cases in which computer code was treated as speech, such as *Universal City Studios, Inc. v. Corley* (2d Cir. 2001); *Junger v. Daley* (6th Cir. 2000); *US v. Elcom* (N.D. Cal. 2002); and *Bernstein v. Dep't of State* (N.D. Cal. 1996).

sufficiently narrowly tailored to satisfy the strict scrutiny standard for **compelled speech**.

- Furthermore, Apple's release of iOS 8 and subsequent versions of iOS included code that placed value on data security and the privacy of customers. Because the government disagrees with this position, compelling Apple to write software contrary to its views amounts to **viewpoint discrimination,** which the First Amendment also prohibits.

Fifth Amendment Substantive Due Process

- Requiring the creation of new software would violate the Due Process clause of the Fifth Amendment because it would deprive Apple of the right to be free from "arbitrary deprivation" of its liberty by government. The order has an "extraordinarily attenuated" connection to the crime, would be highly burdensome to Apple, and would be contrary to Apple's core principles.

Slippery Slope / Unintended Consequences

- As the cryptographers also explained in their paper, it's not possible to create a one-time backdoor tool. Once created, it renders the platform less secure, inviting hackers and foreign governments to find ways to exploit the backdoor to their own purposes, leaving Apple customers less safe and making devices made by companies subject to such laws less popular with consumers as a result.
- Honoring this request would open a Pandora's box of requests from law enforcement both domestic and international, including more repressive governments.
- If a court can order a technology company to write code to bypass security features, what's to stop the government from demanding companies write code to turn on the microphone to aid government surveillance, activate the video camera, or track location?
- To comply, Apple and other tech companies would need to create a dedicated government request digital forensics lab. Who would pay for this?

The Greatest Public Good

- It boils down to a matter of protecting civil liberties. Ensuring robust protection for sensitive customer data protects those customers' civil liberties.
- On balance, a secure communications infrastructure protected by ubiquitous encryption at the device, server, and enterprise level without government monitoring ensures the greatest public good.

CRYPTOGRAPHER CONCERNS

In July 2015 (after the NY smartphone access bill was published and before the San Bernardino attacks), leading cryptographers published a paper detailing the dangers of a law weakening encryption systems, what they called "exceptional access systems."[14]

The authors of the paper identified a number of general problems with an exceptional access regime:

1. It would run counter to a general trend of improving and accelerating internet security. For example, a law requiring backdoors would limit the use of ***forward secrecy***, a relatively new encryption protocol where decryption keys are deleted immediately after use, so that any subsequent theft of the key does not compromise earlier or later communications.
2. Building in exceptional access would substantially increase system complexity, presenting even greater challenges in battle testing software to minimize vulnerabilities.
3. Technologies containing exceptional access systems would act as a sort of hacker honeypot, attracting bad actors intent on leveraging the vulnerability.
4. Mass surveillance would be made more accessible by governments around the world.

The authors provide several examples of how insecure communications technologies designed to comply with government backdoor requirements can be:

1. From 2004–2005, 100 senior members of the Greek government (including the Prime Minister) were wiretapped by unknown parties through the lawful access built into telephone switches owned and operated by Vodafone Greece.[15]
2. Cisco routers configured to permit lawful interception have been deemed insecure by security researchers.
3. The NSA has found all telephone switches built to comply with government-mandated access to be insecure.

In addition to concerns about moving technological innovation offshore, what would it mean for our internet infrastructure if all devices and apps have to include a backdoor? Assuming the U.S. government would regulate app stores for mobile devices, for apps that can be obtained by other means, would the U.S. government institute a national firewall to prevent the use of such apps? In short, the technological consequences of an exceptional access requirement seem endless.

[14] These were many of the same cryptographers who came out publicly against the Clipper Chip proposal in 1997 in a similar paper that many think helped stop that initiative.
[15] *The Athens Affair*, Spectrum, IEEE, vol. 44, no. 7, pp. 26–33, 2007.

A government-run encryption **key escrow system** would present further challenges. Does each government with such a law maintain its own separate escrow, or coordinate with other countries? How do they prevent abuse and compromised encryption keys? Does this create liability for the escrow companies that are assisting these governments?

The presence of exceptional access systems also enables mass surveillance by those with the keys to the system. Would it even be possible, the authors ask, to impose workable limits on this? Recent events suggest it would not.

Finally, would a law requiring exceptional access have an exception for research and teaching? Would it leave room for anonymous communications, which are so vital to a functioning democratic society? None of the legislative proposals put forth so far have addressed any of these concerns.

Clearly legislators need to think carefully about the implications and follow-on effects of any cryptographic legal regime, especially because heavy compliance burdens would be hugely detrimental to technological innovation. For example, the authors argue, had all devices and applications been subject to exceptional access requirements ten years ago, it's doubtful that companies like Facebook and Twitter would exist.

LEGISLATIVE EFFORTS

The FBI's attempt to access Farook's iPhone wasn't the first controversy over government access to encrypted smartphone data. The New York State assembly had introduced a bill requiring similar access in mid-2015. And the California assembly followed suit in early 2016. Finally, as outlined below, the U.S. Congress has also been quite active in attempting to regulate device encryption during the past few years.

NY Smartphone Assembly Bill - June 2015

The New York State Assembly drafted a bill that would have required smartphones sold in the state to be capable of being decrypted or unlocked by the manufacturer or operating system provider. The penalty would have been $2,500 fine per device sold. The bill eventually stalled in committee. We have not seen any renewed interest in it as of the publication of this white paper.

California Smartphone Encryption Bill – January 2016

California lawmakers introduced a similar bill in early 2016, including the $2,500 fine per device sold in the state. This bill also stalled in the face of growing opposition and has not been reintroduced as of the date of publication of this white paper.

Federal Pro-Encryption Legislation

From the pro-consumer, pro-technology side, members of Congress have introduced legislation that would affirmatively *prohibit* the government from forcing private companies to compromise data security: both the House (Rep. Zoe Lofgren) and Senate (Sen. Ron Wyden) introduced their own Secure Data Act of 2015. And the House introduced the End Warrantless Surveillance of Americans Act that same year. In 2016, Rep. Ted Lieu introduced the ENCRYPT bill, which would have preempted state efforts to regulate encryption. Now that the encryption debate has quieted, none of these bills is up for debate.

Burr-Feinstein Bill

Putting to rest any hopes that Congress was entirely pro-encryption, on April 7, 2016, Senators Feinstein and Burr sponsored a bill that would have required “all providers of communications services and products (including software)” to comply with any court order for data (either provide the data or assistance in accessing the data). This would have required Apple, Google, Facebook, and others to engineer backdoors in their products (iOS, Android, WhatsApp). The bill was silent on implementation and technologically illiterate. In addition, it did not appear to anticipate any of the likely knock-on effects passing such a law would entail (see above).

Worse, the bill would have required that distributors ensure the products and services they distribute provide the same access for law enforcement, imposing onerous requirements to vet apps on markets like the Apple App Store and Google Play Store.

The bill was so poorly drafted and ill-informed that many think it helped serve as a rallying cry for the cybersecurity and wider technology community.

LOOKING AHEAD TO 2017 AND BEYOND

Although the Trump administration, Congress, law enforcement, and the state legislatures have been silent on this issue so far, given recent skirmishes at the border there is a good chance that law enforcement will find “urgent need” to compel access to an encrypted device. And the new administration has been clear that it will advocate strongly in favor of requiring access.

What President Trump and the Trump Administration have said so far

- On the campaign trail President Trump said he wanted to expand the country’s surveillance apparatus, and to “err on the side of security.” He said he would support restoring parts of the Patriot Act that have sunset.
- In 2016, Trump was in favor of forcing Apple to provide the FBI with access to the iPhone. Trump had previously advocated boycotting Apple over its refusal to comply with the FBI request.
- CIA Director Mike Pompeo supports the sweeping surveillance program and would like to see the government’s access to communications increase.
- Attorney General Jeff Sessions also supports sweeping surveillance powers like those exercised under Section 215 of the Patriot Act. He likewise supports a diminished USA FREEDOM Act.
- Taken together with Trump’s broader “law and order” rhetoric, these statements suggest that Trump and his administration would strongly favor laws requiring tech companies to unlock their devices.

New York City District Attorney Cy Vance

Manhattan DA Cyrus Vance, Jr. has argued that federal and state governments should have access to every phone in a criminal investigation.[16] In November 2015, his office published, in response to Apple's release of iOS 8 and Google's announcement to follow suit the previous year, a lengthy report on "smartphone encryption and public safety."[17] In that report, Vance and his office proposed what they saw as a solution that balances privacy and safety.

	Device	**iCloud**	**Google Cloud Storage**	**Phone Company**
iMessage content	Yes	No	N/A	No
iMessage metadata	Yes	No	N/A	No
SMS/MMS content	Yes	No	Perhaps	Perhaps
SMS/MMS metadata	Yes	No	Perhaps	Yes
Phone call metadata	Yes	Yes	Perhaps	Yes
Historical cell site data	No	No	Perhaps	Perhaps
Historical other cell tower-related data[18]	Perhaps	No	Perhaps	No
Historical Wi-Fi network data	Perhaps	Yes	Perhaps	No
Historical GPS or other satellite data	Perhaps	Perhaps	Perhaps	No
Contacts	Yes	Perhaps	Perhaps	No
Photos/Videos	Yes	Perhaps	Perhaps	No
Internet search history	Yes	Perhaps	Unknown	No
Third-party app data	Perhaps	No	Unknown	No

[16] No Smartphone Lies Beyond the Reach of a Judicial Search Warrant, N.Y. Times (Feb. 18, 2016).
[17] The report focused solely on full disk encryption (FDE), not encrypted communications in transit.
[18] Some phones capture data about tower signal and other potential towers in the area that the carrier may not have.

The categories of data sources requested by law enforcement is instructive, showing where useful data often resides, and explaining the insistence by law enforcement on access to local data.[19]

Furthermore, the report tells us that there is almost no kind of case in which prosecutors have not used evidence from smartphones. And such evidence is often crucial to the case. Between September 17, 2014 and October 1, 2015, the Manhattan DA's office was unable to execute approximately 111 search warrants for smartphones because they were iPhones running iOS 8, including cases involving homicide, attempted murder, sexual abuse of a child, sex trafficking, assault, and robbery.

Note that defendants cannot be compelled to provide the government with a smartphone password. Such compulsion would violate the defendant's Fifth Amendment rights against self-incrimination.[20]

Cy Vance's Proposed Solution

In his report, Vance proposed a federal or state statute regulating smartphones. In fact, each of the 62 District Attorneys in New York State have supported such legislation. Such a statute, according to the report, would require that "any smartphone manufactured, leased, or sold in the U.S. must be able to be unlocked by the operating system designer. The report goes on to assert that "[c]ompliance with such a statute would not require new technology or costly adjustments. It would require, simply, that designers and makers of operating systems not design or build them to be impregnable to lawful governmental searches."

The report then attempts to address objections (recall that this report was published before the San Bernardino attacks but after the cryptographer paper described above). First, the report questions the need for Apple and Google to throw away the keys in iOS 8 / Lollipop 5 without acknowledging the privacy-invasive events leading up to that change. The report's remaining arguments are no more convincing than that. For example, ignoring the realities of a dedicated hacker community and state actors with countervailing interests, the report suggests that the Fourth Amendment is sufficient to protect personal privacy.

Unfortunately, the report does not explore the implications of such a requirement beyond cursory

[19] Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety, November 2015, p. 7. See the report for more detail on access to these data sources.

[20] See, e.g., *In re Grand Jury Subpoena Duces Tecum*, 670 F.3d 1335, 1346 (11th Cir. 2012). Note that, despite the Fifth Amendment, Vance claims that it's open question as to whether defendants can be compelled to unlock their phone using the passcode.

and conclusory assertions (see the Apple and cryptographer arguments above).

Mr. Vance has been silent on this issue in 2017. But it is unlikely that he and his office have changed their minds about the needs of law enforcement when it comes to smartphone data.

CONCLUSION

Laws like those referenced above pose a threat to technology innovation in America. Were a federal or state legislature to pass a decryption bill, then this technology would likely move offshore and into more open-source software that's not controlled by a single entity, available to only the savviest users.

Furthermore, as Apple argued in its motion to vacate, ensuring robust protection for sensitive customer data protects those customers' civil liberties.

It's too early to say when or whether lawmakers or law enforcement will take a renewed interest in this debate. In this political climate, it's certainly likely that events will reignite this debate at some point in the near future. We will notify our members if legislative activity begins to heat up.

FURTHER READING

1. Apple's battle with the FBI over iPhone security, explained — Vox, February 17, 2016
2. Apple's iOS security guide (May 2016)
3. EFF collection of Apple's motions
4. Timeline of events in the Apple – FBI struggle from The Verge (last updated Sept 16, 2016)
5. Timeline of events from USA Today (March 30, 2016)
6. EFF summary of Trump administration positions on surveillance, encryption, cybersecurity (Dec 2016)
7. Fortune (Feb 26, 2016)
8. How the surveillance state could grow under Trump - Axios (Feb 10, 2017)

9. Keys Under Doormats—a collaboration by the world's top cryptographers warning of the dangers of weakening encryption for law enforcement [PDF] (July 7, 2015)

10. WikiLeaks reveals the CIA hacked into Apple iPhones, Google Android phones and Samsung TVs — recode (March 7)

11. WikiLeaks Reignites Tensions Between Silicon Valley and Spy Agencies — NYTimes (March 7)

12. Why the fear over ubiquitous data encryption is overblown, Mike McConnell, former director of the NSA — Wash Post (July 28, 2015)