Nextgov

Three Reasons Apple's New Encryption Technology is a Good Idea (Even if the FBI Hates It)

Conor Friedersdorf
October 17, 2014

The head of the FBI is upset. In James B. Comey's ideal world, FBI agents would be able to access everything on a person's smartphone as long as a judge had issued a lawful warrant. But technology companies are now selling devices that encrypt the user's data. There is no "backdoor" access. Only the user can decode its contents.

Hence the speech Comey is scheduled to give Thursday. "Mr. Comey will say that encryption technologies used on these devices, like the new iPhone, have become so sophisticated that crimes will go unsolved because law enforcement officers will not be able to get information from them," *The New York Times* reports. "The speech was prompted, in part, by the new encryption technology on the iPhone 6, which was released last month. The phone is the first one that thwarts intelligence and law enforcement agencies, like the National Security Agency, from gaining access to it, even if the authorities have court approval." (The iPhone 6 is not the first smartphone to offer default encryption.)

Comey's speech is part of a sustained effort to sway the debate over encryption, or what the FBI calls devices "going dark," thwarting efforts to solve robberies, kidnapping, and other crimes. Comey has pressed this point on network television:

In the interview that aired on "60 Minutes" on Sunday, Mr. Comey said that "the notion that we would market devices that would allow someone to place themselves beyond the law troubles me a lot." He said that it was the equivalent of selling cars with trunks that could never be opened, even with a court order.

"The notion that people have devices, again, that with court orders, based on a showing of probable cause in a case involving kidnapping or child exploitation or terrorism, we could never open that phone?" he said. "My sense is that we've gone too far when we've gone there."

These concerns strike many people as reasonable. The notion that Apple in particular is behaving badly briefly found purchase with the brilliant legal scholar Orin Kerr. But Comey's arguments are ultimately misleading and wrongheaded, as Julian Sanchez of the Cato Institute explains in a

definitive essay. The full text is worth your while. It begins with a brief sketch of some relevant history:

When the digital world was young, a motley group of technologists and privacy advocates fought what are now, somewhat melodramatically, known as the Crypto Wars. There were many distinct battlefields, but the overarching question ... was this: Would ordinary citizens be free to protect their communications and private files using strong, truly secure cryptography, or would governments seek to force programmers and computer makers to build in backdoors that would enable any scheme of encryption to be broken by the authorities? Happily for both global privacy and the burgeoning digital economy—which depends critically on strong encryption—the American government, at least, ultimately saw the folly of seeking to control this new technology. Today, you are free to lock up your e-mails, chats, or hard drives without providing the government with a spare key.

I'd add that you've long been free to buy a safe that opens only with your thumbprint, bury a treasure chest in a location known only to you, or write a diary in code. Jumping to the present, Sanchez debunks the notion that Apple or anyone else is setting an alarming new precedent with its encryption:

It is Apple's backdoor access that was the aberration, even for Apple. If you encrypt your MacBook's hard drive with Apple's FileVault, or your Windows computer with Microsoft's BitLocker, then unless the user chooses to send either company a backup copy of her encryption key, they can no more unlock those encrypted files than a bookbinder can decipher the private code you employ in your personal diary. Strong encryption is not even new to smartphones: Google's Android operating system—the world's most popular mobile platform, running on twice as many devices as iOS—has featured full-device encryption since 2011, and Google has never had backdoor access to those encrypted files. And, of course, there have always been a wide array of third-party apps and services offering users the ability to encrypt their sensitive files and messages, with the promise that nobody else would hold the keys.

Acknowledging that encryption may nevertheless be growing easier and more prevalent, in a way that will sometimes thwart law enforcement from solving crimes, Sanchez shows that the case against backdoors for law enforcement is nevertheless strong.

This is so for three reasons:

1. "A backdoor for law enforcement is a *deliberately introduced security vulnerability*, a form of architected breach: It requires a system to be designed to permit access to a user's data against the user's wishes, and such a system is necessarily less secure than one designed without such a feature .... Activist Eva Galperin puts the point pithily: 'Once you build a back door, you rarely get to decide who walks through it.' Even if your noble intention is only to make criminals more vulnerable to police, the unavoidable cost of doing so in practice is making the overwhelming majority of law-abiding users more vulnerable to criminals."
2. "Authoritarian governments, of course, will do their best to prevent truly secure digital technologies from entering their countries, but they'll be hard pressed to do so when

secure devices are being mass-produced for western markets. An iPhone that Apple can't unlock when American cops come knocking for good reasons is *also* an iPhone they can't unlock when the Chinese government comes knocking for bad ones. A backdoor mandate, by contrast, makes life easy for oppressive regimes by guaranteeing that consumer devices are exploitable by default ..."

3. While Apple may tightly integrate its hardware and software, most device manufacturers don't. By creating a legal obligation to help police to access devices, "you necessarily encourage them to centralize control over the software running on that device ... there's not much point in requiring Google to release an insecure version of Android if any user can just install a patch that removes the vulnerability .... In the long run, the options are an ineffective mandate that punishes companies that choose centralized models, or a somewhat more effective mandate that will still be circumvented by sophisticated criminals … but only at the cost of destroying or marginalizing the open computing architectures that have given us decades of spectacular innovation."

Sanchez concludes by observing that while default encryption may cause the FBI to lose some access it previously enjoyed to criminal communications, it is misleading to view that loss outside a larger context in which everyone, including criminals, create a once-unimaginable trail of their activities.

With regard to Apple alone, "The company's ecosystem considered as a whole provides a vast treasure trove of data for police even if that trove does not include backdoor access to physical devices. The ordinary, unsophisticated criminal may be more able to protect locally stored files than he was a decade ago, but in a thousand other ways, he can expect to be far more minutely tracked in both his online and offline activities. An encrypted text messaging system may be worse from the perspective of police than an unencrypted one, but is it really any worse than a system of pay phones that allow criminals to communicate without leaving *any* record for police...? Meanwhile activities that would once have left no permanent trace by default—from looking up information to moving around in the physical world to making a purchase—now leave a trail of digital breadcrumbs that would have sounded like a utopian fantasy to an FBI agent in the 1960s."

I'd only add that, even ignoring all these benefits of backdoor-free encryption, the practice is necessary as a response to a federal government that routinely intrudes into the private communications of Americans suspected of no crime, rather than respecting privacy except in cases where an individualized warrant is obtained. Perhaps if the Bush administration hadn't embarked on an illegal program of warrantless wiretapping, if the telecoms wouldn't have been given retroactive immunity for their unlawful behavior, and if Edward Snowden hadn't shown that U.S. officials lied under oath about a program of mass surveillance, Americans would feel less need to build safes that not even the state can unlock.