To Break or Not to Break Encryption: The Global Debate

The FBI and others battle with keeping both the nation, and privacy citizen data, safe.

Amanda Ziadeh

Wed, 11/28/2018 - 15:35

FBI Director Christopher Wray answers questions from the press. (FBI photo)

In the name of national security, governments are starting to consider encryption backdoors that would allow law enforcement to get to the secure data of criminals — but does this put the integrity of encryption itself, and the companies vowing to secure customer data, at risk?

Earlier this year, Australia’s government drafted an Assistance and Access Bill (still being deliberated) that would require companies to cooperate with security agencies looking for access to encrypted data, The Guardian reported. The bill appears to allow law enforcement to require companies like Facebook and Google to retain user metadata.

What’s been dubbed an “encryption-busting bill” by ZDnet for its potential to create backdoors and access to encrypted content, has caused controversy around safeguarding customer data while ensuring national security, and it’s not only a conversation Australia is having.

In the U.S., FBI Director Christopher Wray testified before Congress in December referring to the FBI’s “Going Dark” challenge; the gap between law enforcement’s legal ability to access digital information, and its technical ability to do so.

In his testimony Wray said, “we are seeing more and more cases where we believe significant evidence resides on a phone, a tablet, or a laptop . . . If we cannot access this evidence, it will have ongoing, significant effects on our ability to identify, stop, and prosecute these offenders.”

Wray said the FBI doesn’t intend to expand the government’s legal authority, but wants to ensure it can obtain the electronic information needed for evidence to keep the nation safe.

But is there Traction?

According to Congressman Jim Himes (D-Conn.), ranking member on the National Security Agency and Cybersecurity Subcommittee on the House Permanent Select Committee on Intelligence, there really isn’t much legislative momentum in the U.S. around the idea of a backdoor, largely due to privacy concerns on both sides of politics.

There’s a “growing realization that if you deliberately create vulnerabilities, nobody is safe,” Himes said at the Nov. 27 New America event in Washington, D.C. The government relies on encryption to keep sensitive national security information safe, so it’s understandable as to why someone like Adm. Michael Rogers, director of the NSA, for example, would appreciate strong encryption.

And perhaps why others would have a different perspective on the subject, such as James Comey, former FBI director, “who really wants to break into that iPhone in San Bernardino,” Himes said.

But the idea that there should be a deliberate vulnerability allowing only the “good guys” to access someone’s personally identifiable information doesn’t sit well with most, Himes added.

“If you legally require American technology companies to provide extraordinary access to the U.S. government, well what about the Chinese government?” Himes asked. If the vulnerability is there, the bad guys can get in, too.

There are also legal concerns associated with government requiring the construction of a product designed to pick a lock, as Himes put it, which can also damage the strength of a company’s other products.

And rather than asking for backdoors, Himes said law enforcement and intelligence agencies should use their monetary resources to keep up with technology, not stop it.

“I want the NSA to really think hard about how to crack encryption, because I want them to do that, but that doesn’t necessarily mean the answer, of course, is to create a technical vulnerability,” Himes said.

An Outsider’s Perspective

Robert Anderson, former FBI Executive Assistant Director for the Criminal, Cyber, Response, and Services Branch which oversaw all criminal and cyber investigations, has had a change of heart since leaving law enforcement — a field he spent nearly 31 years in — and joining the private sector three years ago. Anderson currently serves as principal at security delivery company The Chertoff Group.

“In the last couple years, my perspective on encryption as it pertains to data inside the private sector has dramatically changed from when I was the number three or four guy in the FBI,” Andersons said at the New America event.

His first real experience with major cyberencrypted data theft was during the Edward Snowden investigation, which he ran from the day it started. What surprised him most was that “not one single solitary alarm bell went off in one of the most sophisticated technical organizations in the world,” he said, and this event set the stage for how important, and damaging, cyber was becoming.

A few years later, Anderson was in charge of the 2015 San Bernardino, Calif. attack investigation. This particular incident triggered controversy over the FBI's attempts to obtain information off an encrypted iPhone belonging to the terrorist.

The FBI received a court order to demand that Apple write special software to bypass the security feature that erases the phone's content if someone gets in, NPR reported. Apple refused and took the FBI to court, arguing that this kind of "master key" software could entice other countries to make similar demands for other iPhones. In the end, the FBI paid a third party to unlock the phone without Apple.

But from within the FBI, Anderson said himself and other leaders were consumed with trying to get the phone data in order to stop another potential attack.

"It was met by huge resistance," Anderson said, "and from where I stood then, I didn't really understand it."

That's because for the entirety of his career in law enforcement, the FBI would go to court, a federal or state judge would issue a subpoena, and the FBI would provide that subpoena to get the information it needed.

"This was one of the first times I could ever remember . . . that we couldn't get the information, and I really didn't understand it," Anderson said. But since joining the private sector in January 2016, his perspective has dramatically changed.

Consumer Trust

Anderson's industry career began with running a global information security practice, responsible for stopping 2,000 breaches in those nearly three years, for U.S. companies and their bases abroad.

Anderson said the one thing that stuck out to him immediately was the fiduciary responsibility these companies had and were being entrusted by clients to do: protect their information and keep data safe.

"After all the breaches that I've been involved in in the last three years, I do think that opening backdoors to some of this technology is worse off for the people, the clients that have employed these private sector businesses, then it would be to somehow work through how we would get that maybe without that type of data needed," Anderson said.

This perspective of just how much client data private companies are protecting didn't occur to him during his time with the FBI. He said he was looking at it through a myopic glass, and changes need to be made so that the FBI and industry will start to have conversations about encryption and encrypted data.

"I really believe we're kind of stuck . . . in a loop that started back in 2015," he said.

And though the pressure from law enforcement and the intelligence community to stop what was believed to be another potential attack during the San Bernardino shooting surrounded the FBI at the time, Anderson said looking back, he's not confident that the FBI couldn't have gotten the information they needed from another venue.

Changing the Conversation

Considering the U.S. has thousands of dispersed police forces nationwide, Anderson said one of the biggest problems is that the government isn't having the necessary conversations collectively and with companies to find ways of not intruding on the consumer data they protect. It starts with educating all the law enforcement officers across the country in other ways to harvest that data.

Outside the major metropolitan police forces, cyberexpertise begins to degrade, Anderson said. And not because they can't learn, but because of the technology being used to get information through social media and open source events; the same information that the FBI relied on subpoena power to obtain.

To educate, Anderson suggested Congress allocate funding for federal, state and local law enforcement, and to private sector, to provide the training needed. Technology-related training changes often, and some agencies don't have the budget to keep up.

"I honestly don't think that conversation has been had," Anderson said, and in fact, the FBI may be missing the point.

For example, to explain the types of problems encrypted content creates, the FBI claimed investigators were locked out of 7,800 devices that were connected to crimes last year, when it was found that the number is more likely between 1,000 and 2,000, according to The Washington Post.

But aside from this inflated number, Anderson said the FBI shouldn’t count how many encrypted cell phones, computers or apps there were, but rather, out of all encrypted content and devices, how many of these items actually prohibited the FBI from getting the information it needed in some other way.

For example, it may mean law enforcement asking companies what is off limits due to their fiduciary responsibilities to the clients. From an FBI perspective, Anderson said he’s never heard these kinds of conversations before because typically, when there is probable cause, it’s enough for the FBI to go to a federal judge and obtain a subpoena.

And that’s the conversation Anderson said is missing around encryption. Industry and government will be sharing this space, as technology is not going to go backwards. And since San Bernardino, “there’s been no clear way to delineate the lines on how we’re going to look at this as a country, as a nation and as intelligence services around the U.S.,” Anderson said.

But these conversations may have to be in the theoretical, considering there’s no real way to predict the extent, pace and impact of cyber and encryption advancements. Theoretical conversations can help law enforcement and industry understand and prepare for just how far encryption and the challenges it brings can go, to form a collective conversation around how to protect the nation and citizen data.

View PDF
FBI
Congress
encryption
NSA
Apple