SCHOLARS
STRATEGY NETWORK

How to Think about Access by Law Enforcement to Encrypted Electronic Data

Alan Zachary Rozenshtein, University of Minnesota-Twin Cities

In 2016 the FBI demanded that Apple help it access the encrypted iPhone belonging to a perpetrator of a mass shooting in San Bernardino, California. When Apple refused, the fight between the government and Silicon Valley made national headlines. Ultimately, the FBI backed down after buying a hacking tool from a third party. But the larger issue — government access to encrypted data — is anything but resolved.

The Government's "Going Dark" Problem

Federal, state, and local law-enforcement agencies argue that their investigations are "going dark" because the evidence they need is often encrypted. Although commercial encryption has been available for decades, technology companies have in the last few years seamlessly built it into their biggest products. For example, Apple's iOS devices and WhatsApp's messaging service both automatically encrypt data in a way that prevents even the companies from accessing it. Consequently, even when law enforcement gets a warrant or a court order to search a device or read electronic messages, it is unable to do so; and because of the ways the products are designed, the companies that make them cannot help government gain access.

The "going dark" problem is growing. In 2017 alone, the Manhattan District Attorney's Office and FBI reported being unable to access hundreds and thousands of encrypted devices, respectively. The number of devices they cannot access will only increase going forward. Although there are a variety of third-party tools that can get around encryption, especially for older devices, they do not cover all products and are too expensive to be used regularly. For small local police departments that investigate the vast majority of crime, these tools might be too expensive to use at all. Given the growing problem of blocked access to electronic data, law-enforcement agencies both at home and abroad are increasingly calling for legislation that would require companies to design their encryption systems to provide "third-party access" to the government on (typically court-authorized) demand.

The Dangers of Weak Encryption

Just as too much encryption can harm public safety, so can too little. Encryption safeguards the privacy and personal information of device users, allowing them to communicate securely with others. Encryption enables a mass of both on- and off-line economic activity. Unfortunately, an encrypted system that allows third-party access (for example, by the government) would likely be less secure than one that does not allow third-party access. The more entities that can decrypt data, the more opportunities there are for a bad actor to access that data. In addition, a system that allows for third-party access is also more complicated than a system without such access. This is especially true for systems that would have to work across the globe. For example, it would be difficult to design a system that would simultaneously give access to law enforcement officials in

the United States and Russia without at the same time exposing one country's citizens up to the risk of surveillance by the other country's government.

These challenges may not be insurmountable. Even if third-party access has some unresolvable security risks, they may be acceptable. Tradeoffs are inevitable when clashing principles must be balanced. But the stakes are enormous, and, if not handled carefully, the cure of authorized third-party access to encrypted data may prove worse than the disease of diminished law enforcement.

The Path Forward

My research on the topic suggests there are several things that can be done to ensure the conversation about government access to encrypted data moves in a productive direction:

- Easy answers — those that offer a simple solution or pretend the problem does not exist — should be rejected. For example, the government has argued that Silicon Valley should design their encrypted products to permit government access. But the government has not put forward a concrete proposal as to how to design such a system, or even demonstrated it is possible. On the other side of the debate, some argue that far from "going dark," the government is enjoying a "golden age of surveillance" and data from other sources will make up for encrypted content the government cannot access. But this argument ignores the fact that data are not fungible and government's legitimate need for access to prevent or solve crimes is steadily growing.
- Instead of focusing on ideal, illusory solutions, attention should focus on imperfect but attainable goals. For example, many security researchers advocate "lawful hacking," by which the government would exploit existing vulnerabilities in hardware and software rather than forcing manufacturers to design new vulnerabilities. However, reliance on lawful hacking requires acknowledging that this approach might be too difficult or expensive to use in many investigations. This approach could also encourage government to hoard rather than disclose its knowledge of vulnerabilities, undermining trust with the technology community.
- The government should develop two kinds of new knowledge. Authorities should collect detailed statistics on the extent to which encryption hampers law enforcement. And they should fund research and production of secure encrypted systems that provide government access — much as, in the 2000s, the Defense Department used "Grand Challenges" investments to develop autonomous vehicles.
- The government needs to rebuild its relationship with the technology community, a relationship that has been undermined by various developments, including Edward Snowden's 2013 disclosures about government surveillance. The government should establish programs to allow members of the technology community to work collaboratively with law-enforcement agencies. And authorities should avoid tactics that needlessly provoke the technology community — including asking for court orders to force companies to build "backdoors" into their products and promoting legislation to outlaw certain forms of encryption.

Together, these suggestions will put the conversation about government access to encrypted data on a more constructive path. That is, of course, does not guarantee a solution, but, when it comes to solving complex, intractable dilemmas, constructive conversations are often the way forward.

Read more in Alan Z. Rozenshtein, "Wicked Crypto", *UC Irvine Law Review* 9 (2019).