Insight

Return of the Cryptowars: Why Encryption Matters for Data Privacy and Data Security

JENNIFER HUDDLESTON | MARCH 10, 2020

Executive Summary

- Encryption technology has beneficial cybersecurity implications for individuals, businesses, and even the military.
- Even if only intended to target bad actors, "backdoors"—built-in changes to technology that allow access to encrypted information—would create vulnerabilities that undermine many benefits of encryption.
- The U.S. government often already has means of accessing encrypted technology, and instead of creating risky backdoors, it should focus on encouraging law enforcement agencies to use the tools already at their disposal as well as focusing more directly on the underlying illegal behavior.

The Debate Over Encryption

Popular apps with billions of users, such as WhatsApp and Signal, secure their messages through encryption technology. Industries such as finance and medicine, and even the U.S. military, rely on encryption to secure sensitive data. Despite these beneficial and common uses, policymakers and others are concerned about how these technologies could be abused by bad actors, whether terrorists seeking to shield their communication from surveillance ("going dark") or people sharing illegal content. The battle between the Federal Bureau of Investigation (FBI) and Apple over accessing the iPhone of one of the San Bernardino shooters is a well-known example of the tensions that arise because of encryption.

These long-simmering debates over encrypted communications and law enforcement's access to them are heating up again because of the recently introduced EARN IT Act and various statements from Attorney General William Barr. Advocates for law enforcement "backdoors"—built in technological changes that provide access to otherwise secure information—argue they are needed to prevent "lawless spaces," but such changes would bring consequences to cybersecurity, privacy, and civil liberties as well as the economic benefits of innovation. Far from being only a tool for those with something to hide, encryption benefits a wide range of users by offering an accessible way to improve security and privacy. Policy changes that risk undermining the security of this technology must be considered beyond their impact on worst-case scenarios.

Why Encryption Matters

Far from just being used by those with malicious purposes, encryption provides many benefits to average individuals, businesses, government, and the military. More consumers and businesses are using various encrypted services for improved data privacy or security. The 82nd Airborne of the U.S. Army is reportedly using an encrypted messaging service, Signal, to communicate rather than risk interception by adversaries of the information through standard telecommunications options. Reporters use encrypted messaging to communicate

with sources for whom interception of messages could put them at risk, and protesters in autocratic regimes have used encryption to organize protests. Businesses may use encryption to protect intellectual property or personally identifiable information from potential hacks. And encrypted messaging is increasingly popular with the general public via apps like WhatsApp, Signal, and Telegram.

Encryption provides key options for those businesses or individuals that prefer a more privacy-centric or secure choice for communication or protecting their data. Companies such as Apple and Facebook are responding to increasing market demands by providing "end-to-end" encryption for messaging, meaning messages can only be read in their decrypted form by the sender and therefore less vulnerable to third party interception during transmission.

The diverse range of consumer privacy preferences ideally results in a market with many different privacy options, and in some cases end-to-end encryption can serve the needs of those who highly value data privacy or have sensitive data such as medical or financial information. As a Carnegie Endowment For International Peace white paper notes, "The importance of encryption has grown as information technology enables the creation and storage of more and more sensitive personal information. User-controlled encryption is and will be in the future an essential component of delivering on those desires, particularly as individuals become more skeptical of U.S.-based and foreign technology companies." In this way, encryption technology empowers individuals to act in accordance with their privacy preferences and for companies to respond to market demands.

Weakening encryption options while many are calling for increased privacy restrictions or heightened data security could limit existing options. Encryption is a tool, and like most tools, there is always a possibility that bad actors could use it to engage in harmful behavior. But given the numerous potential benefits of encryption, the consequences and tradeoffs of policies that might undermine key elements reach well beyond bad actors.

The Problem of Backdoors

The current debates about encryption are not the first time that law enforcement and innovators have clashed over the technical components of secure communications technology. Looking at these prior debates, the potential pitfalls to security of backdoors becomes clearer. These past "Crypto Wars" also illustrate the many potential tradeoffs associated with policies that weaken encryption.

In the 1990s, for example, government and law enforcement were concerned about such technology, and so they sought backdoors via the proposed insertion of the "Clipper Chip." This additional chip would have been required by the government to be included in certain technologies and would have created a way for law enforcement and intelligence agencies to access encrypted communications without denying the public access to encryption tools. During these earlier debates, vulnerabilities in the system were discovered that could allow the technology to be breached and exploited by adversarial outsiders. As a result, the Clipper Chip was never added to cell phones.

The same fear exists today. There are concerns about how such backdoors could create opportunities for surveillance and potential violations of civil liberties, if not by the U.S. government then by oppressive or adversarial regimes able to exploit such technical requirements. As Apple CEO Tim Cook said of proposed law enforcement backdoors, "any back door means a back door for bad guys as well as good guys." A backdoor cannot be created for just one entity without risking its exploitation especially given the rise in attempted cyberattacks.

But security risks are not the only potential consequence of weakening encryption. For example, creating a backdoor could have economic impacts by Further, domestically creating a backdoor might limit the tools and services that provide protection for businesses in fields handling sensitive data, such as medicine or finance.

Such concerns show how debates about backdoors also are relevant to ongoing policy conversations around data privacy and cybersecurity. While much of the data privacy debate centers around consumer choices and privacy options of private companies, there are also important conversations around ensuring civil liberties in the digital age. Encryption serves an important role in multifaceted privacy debates. It can provide an important tool for those concerned about potential government surveillance, and with the rise of numerous encrypted services it can also provide an easily accessible option for those who want greater privacy. Yet, a backdoor could undermine these key benefits not just for those with malicious intent but for average consumers and businesses.

Alternatives for Addressing Bad Actors Using Encrypted Technology

Law enforcement continues to express concern about its ability to respond to crimes coordinated through encrypted technology. The good news for those concerned about public safety is there are other options beyond backdoors that can enable law enforcement to access necessary evidence such as locked iPhones. For example, following the FBI-Apple dispute over one of the San Bernardino shooters' iPhone, the Department of Justice's Office of the Inspector General indicated there were other feasible ways of gaining access to such a device without the creation of a backdoor, but the agency pushed forward to litigate the issue without pursuing these other options first.

A 2017 paper from the Center for Strategic and International Studies discussed the "low hanging fruit" of digital evidence and how the greatest challenge facing law enforcement is not the inability to access digital evidence but the ability to identify and utilize such evidence effectively. An alternative policy solution to creating backdoors would be twofold: provide law enforcement better training and resources on using existing digital technologies, and respond more narrowly to illegal online behavior such as child sexual exploitation, as TechFreedom's Ashkhen Kazaryan has pointed out. Tech companies already report such illegal activity to the National Center for Missing and Exploited Children and have continued to develop tools to help better identify and remove such content. To help law enforcement respond to these specific concerns, policymakers could increase resources and training rather than creating a backdoor that could undermine the benefits of encryption technology to other consumers and businesses.

While law enforcement should not be unnecessarily handicapped, existing tools, including the ability to collaborate with internal and external experts to get into locked devices and the ability to obtain necessary digital evidence through proper legal channels, can enable access in extreme cases without weakening the benefits or threatening civil liberties. Law enforcement should have the resources to address concerns about illegal activity, including those conducted via encrypted technologies. In providing these tools, however, policies should not create greater risk that undermine security and civil liberties. Rather than creating a risky and expansive policy by requiring a backdoor, policymakers and law enforcement should seek to better use existing tools and to focus on the underlying problematic behavior.