Unlocking Encryption: Information Security and the Rule of Law

EXECUTIVE SUMMARY

BY DANIEL CASTRO AND ALAN MCQUINN | MARCH 2016

The widespread adoption of encryption among consumers and businesses has created one of the most difficult policy dilemmas of the digital age. Simply put, advances in encryption have vastly improved information security for consumers and businesses but also made it harder for law enforcement and national security officials to prevent and investigate crimes and terrorism.

This report examines the nuances of the debate over encryption and concludes that governments should not restrict or weaken encryption, because any attempts to do so would reduce the overall security of law-abiding citizens and businesses, make it more difficult for companies to compete in global markets, and limit advancements in information security. Moreover, attempts to restrict or weaken encryption would be ineffective at keeping the technology out of the hands of many criminals and terrorists. Therefore, the report offers a series of recommendations to encourage greater information security around the world.

The Debate Over Encryption

The debate over encryption has gained more attention recently as some law enforcement agencies have complained about their lack of access to data. These complaints have been spurred by decisions that some mobile and cloud-based service providers have made to upgrade their security controls so that their customers can retain the keys used to encrypt their data, thereby locking out third parties, including law enforcement.

However, these complaints are not new. The past few decades have seen a steady stream of advancements in encryption, and many companies have integrated encryption into popular products and services to improve security for users. Some government agencies have pushed back on these kinds of improvements, citing law enforcement and national security concerns. But while advances in encryption, along with more widespread adoption, certainly will make it harder than it is today for law enforcement and intelligence agencies to access some kinds of data, the overall impact on fighting crime and terrorism will be difficult to measure.

Methods for Accessing Encrypted Data

There are multiple methods that governments can use to gain access to information that users might protect with encryption. These options include banning strong encryption, prohibiting client-side encryption, mandating key escrow, weakening encryption standards, creating software and hardware backdoors, hacking into private systems, and using traditional investigative techniques.

Some of these methods involve breaking encryption, some involve circumventing it, and some involve gaining access to the keys. Each of these methods involves different levels of security risk and reliability for law enforcement and intelligence agencies. But any proposal to weaken or limit encryption would weaken cybersecurity.

Proposals and Justifications for Accessing Encrypted Data

The intelligence community and law enforcement have made five principal arguments for why policymakers should limit or weaken encryption. Each of these arguments is flawed or limited:

First, they argue that companies should not offer technology that circumvents established legal requests, cautioning that "warrant-proof encryption" is interfering with law enforcement's long-standing ability to conduct lawful searches. However, law enforcement officials have never had the ability to read properly encrypted information. While the scale of the impact of encryption on law enforcement is much greater today than in the past, the phenomenon itself—the inability of law enforcement to access encrypted data when the user controls all of the keys—is not new.

Second, they argue that without access to encrypted data, the government will be less able to stop or solve crimes and terrorism. This is true, and these problems will be exacerbated if law enforcement and the intelligence community do not develop or use new tools and techniques for an age of secure digital communications. However, limiting encryption is not the right answer, because it will create systemic cybersecurity vulnerabilities. Unlocking encrypted data is not the only way to investigate crime or prevent terrorism. Moreover, regardless of what laws the United States puts in place, it cannot stop terrorists or sophisticated criminals from encrypting data anyway.

Third, they say companies have decided to stop retaining a copy of their customers' encryption keys for business reasons alone. This is simply not true. Companies have done this because allowing users to control their own keys increases security and allows them to better manage risk.

Fourth, they argue that technologists could create a way for the government to access encrypted data without compromising security if they simply tried harder to solve the problem. Unfortunately, encryption is based on math, not magic, and there is no way to create third-party access for the government without introducing vulnerabilities that could be abused by adversaries.

Finally, they say that companies should help law enforcement hack into the products they sell so that the government can gain access to users' encrypted data. But if this technique

were abused, then law-abiding users might begin to distrust these companies and refuse to adopt their products or install their software security updates, thereby creating harmful unintended consequences. Certainly, companies should comply with lawful government requests to the extent they are able. But to prevent abuse, government requests for assistance from the private sector should occur only under limited circumstances and with strong judicial oversight. In addition, the government should not restrict companies from designing products with security features that cannot be defeated, even by the company.

Impact of Limiting Encryption

Any decisions to weaken or limit encryption will have harmful effects on the overall digital economy, including making digital systems more vulnerable; increasing costs for consumers (as risks increase and companies pass on greater operational expenses); decreasing competitiveness of U.S. businesses seeking international market share; and diminishing U.S. leadership in setting policies to improve cybersecurity.

Recommendations

Rather than place barriers on encryption, the U.S. government should advocate for better cybersecurity practices both domestically and abroad, in part by encouraging continued innovation in encryption. Congress and the administration can do so by rebuilding trust in the U.S. tech sector through strong data security practices at home, providing law enforcement with new tools to uphold the law, and projecting the United States' firm commitment to data security to the world.

Specifically, Congress and the administration should pursue the following policies:

- Congress should bar the National Security Agency from intentionally weakening encryption standards and strengthen transparency in the cryptographic standards-setting process.
- Congress should pass legislation banning all government efforts to install backdoors into companies' products and services or to require companies to facilitate government access by altering the design of the systems they sell. Legislation also should preempt states' actions on these issues.
- Congress should pass legislation requiring all federal agencies that discover security flaws in commercial and open-source products and services to disclose them in a timely and responsible manner, and to work with private industry to fix them.
- Congress should examine whether U.S. courts can better balance the interests of the individual and the state by allowing law enforcement to hold suspects in contempt of court for failing to disclose keys to their own encrypted data.
- Congress should provide additional resources for federal, state, and local law enforcement to investigate and analyze digital evidence in a way that is suitable for presentation in a court of law.

- Congress should establish clear rules for how and when law enforcement can hack into private systems, and how and when law enforcement can compel companies to assist in investigations.

- U.S. trade negotiators should oppose foreign governments' efforts to introduce backdoors in software or weaken encryption, including rules to require companies to sell products with weak encryption.

- The U.S. government should promote cybersecurity around the world by championing strong encryption in global Internet and technology policy forums.

ACKNOWLEDGMENTS

The authors wish to thank the following individuals for providing input to this report: Robert Atkinson, Randolph Court, and Bruce Heiman. Any errors or omissions are the authors' alone.

ABOUT THE AUTHORS

Daniel Castro is vice president of ITIF. His research interests include health IT, data privacy, e-commerce, e-government, electronic voting, information security, and accessibility. Before joining ITIF, Castro worked as an IT analyst at the Government Accountability Office where he audited IT security and management controls at various government agencies. He has a B.S. in Foreign Service from Georgetown University and an M.S. in Information Security Technology and Management from Carnegie Mellon University.

Alan McQuinn is a research assistant at ITIF. His research areas include a variety of issues related to emerging technology and Internet policy, such as cybersecurity, privacy, virtual currencies, e-government, and commercial drones. Prior to joining ITIF, McQuinn was a telecommunications fellow for Representative Anna Eshoo (D-CA) and an intern for the Federal Communications Commission in the Office of Legislative Affairs. He got his B.S. in Political Communications and Public Relations from the University of Texas at Austin.

ABOUT ITIF

The Information Technology and Innovation Foundation (ITIF) is a nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized as one of the world's leading science and technology think tanks, ITIF's mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress.

FOR MORE INFORMATION, VISIT US AT ITIF.ORG.