FEBRUARY 2017

# The Effect of Encryption on Lawful Access to Communications and Data

AUTHORS
James A. Lewis
Denise E. Zheng
William A. Carter

A REPORT OF THE
CSIS TECHNOLOGY POLICY PROGRAM

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

ROWMAN & LITTLEFIELD
Lanham • Boulder • New York • London

—-1
—0
—+1

# About CSIS

For over 50 years, the Center for Strategic and International Studies (CSIS) has worked to develop solutions to the world's greatest policy challenges. Today, CSIS scholars are providing strategic insights and bipartisan policy solutions to help decisionmakers chart a course toward a better world.

CSIS is a nonprofit organization headquartered in Washington, D.C. The Center's 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look into the future and anticipate change.

Founded at the height of the Cold War by David M. Abshire and Admiral Arleigh Burke, CSIS was dedicated to finding ways to sustain American prominence and prosperity as a force for good in the world. Since 1962, CSIS has become one of the world's preeminent international institutions focused on defense and security; regional stability; and transnational challenges ranging from energy and climate to global health and economic integration.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in November 2015. Former U.S. deputy secretary of defense John J. Hamre has served as the Center's president and chief executive officer since 2000.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

# Acknowledgments

This report is made possible by the generous support of the Smith Richardson Foundation and BSA | The Software Alliance.



ISBN: 978-1-4422-7995-7 (pb); 978-1-4422-7996-4 (eBook)

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.**csis**.org

Rowman & Littlefield
4501 Forbes Boulevard
Lanham, MD 20706
301-459-3366 | www.**rowman**.com

-1—
0—
+1—

# Contents



—-1
—0
—+1

# Executive Summary

It is in the national interest to encourage the use of strong encryption. No one we interviewed in law enforcement or the intelligence community disagreed with this. The crux of the problem is whether to restrict instant messaging and full disk encryption that does not allow for recovery of unencrypted data without the consent of the user. These are fast-growing market sectors, and decisions by a few companies will have a profound effect on type and prevalence of encrypted communications.

While encryption use is growing rapidly, the share of traffic that is both of interest to law enforcement and unrecoverable is still relatively small. Most companies use encryption that allows law enforcement agencies to recover plaintext data. Most e-mail, if it uses encryption, also allows for recovery. Currently, an estimated 18 percent of global communications traffic is end-to-end encrypted. It is estimated that 22 percent of communications traffic will be end-to-end encrypted by 2019. About 47 percent of all mobile devices in the United States have full disk encryption. If all iOS and Android devices adopt full disk encryption, about 99 percent of the world's smartphones could become inaccessible to law enforcement.

Comprehensive data on how frequently federal and state law enforcement encounter unrecoverable encryption is unavailable, so it is unclear how damaging increased encryption use is for law enforcement. Access to end-to-end encryption makes investigations difficult. However, it is unclear if increased encryption use leads to an increase in crime. Publicly available material on major terrorist attacks reveals that terrorists distrust Western encryption and rely on burner phones, couriers, or prearranged codes to evade surveillance.

Other countries have concerns about encryption and many favor restrictions, including democracies like Brazil, France, and the United Kingdom. China and Russia already use a range of techniques to ensure that they maintain access to data and communications. While a majority of countries would favor some kind of restriction on access to unrecoverable encryption, there is no global consensus, and the likely outcome is a hodgepodge of national policies.

Our research suggests that the risk to public safety created by encryption has not reached the level that justifies restrictions or design mandates. The encryption issue law enforcement faces, while frustrating, is currently manageable. Alternatives to restriction include international cooperation, expanded use of data analytics, improved law enforcement access capabilities, and regional decryption labs. Such solutions are imperfect, but they face fewer political obstacles than restriction. Law enforcement agencies fear that this situation could change rapidly for the worse, but interim solutions that improve law enforcement's technical capabilities can provide time to identify sustainable national and international policies on encryption.

01

# Introduction: Encryption's Effect on Lawful Access to Communications and Data

Technological innovation creates powerful forces for change to which societies must adjust. A series of events—the May 2013 Snowden revelations, growing concern about cybersecurity, and the adoption of new privacy features in consumer devices and applications—has changed how people think about encryption. Encryption has enormous benefits for security and privacy, and the use of encryption by individuals and organizations should be encouraged. The challenge comes from devices, applications, and services that provide encryption that is impossible to access without the assistance of the user, and the impact of this on public safety.

Encryption scrambles plaintext messages. It turns data into unreadable code that can only be deciphered by those that have a secret key or password. Some encryption products and services allow a third party to provide access to decipher encrypted communications without the cooperation of the sender or recipient of the message, or the owner of the device on which the encrypted data is stored. We call this "recoverable" encryption. These recovery mechanisms can be used to provide unencrypted data to law enforcement agencies in response to a warrant. "Unrecoverable" encryption products and services use cryptographic techniques that prevent any third party, including the service provider, from being able to read the encrypted communications, even with a valid court order. It is this unrecoverable encryption that causes the greatest challenge for law enforcement.

Those who fear government surveillance worry that restrictions on encryption will put their privacy at risk. At the same time, there is growing risk to public safety as organized crime, terrorists, and child pornographers are drawn to the use of encrypted communications platforms that are technically impossible to access by law enforcement or by the companies that provide the devices and applications. Cybersecurity adds a further complication, because the need to protect data from cybercriminals and spies means that the national interest is best served by increased use of encryption. Societies must choose how to balance privacy, cybersecurity, and public safety to decide whether increased use of unrecoverable encryption creates risks that justify regulation of its design, sale, or use.

## ENCRYPTION POLICY IS OUT OF DATE

The current debate builds on earlier experience. In 2000, the United States removed restrictions on the sale of strong encryption[1] even though it knew this could harm law enforcement and intelligence collection. The reasoning in 2000 was that letting companies and consumers use strong encryption on the newly commercialized Internet would make it safer, and the nation would gain economically and in security.

However, few people or organizations took advantage of encryption in 2000. At that time, using encryption involved complications, expense, and delays. As a result, the effect on law enforcement and intelligence was much smaller than expected. Today's different technological and security environment requires a reexamination of the 2000 decision.

Even though strong encryption was made available in 2000, most people did not use it, and most of the encryption products on the market were recoverable. Now, strong encryption is inexpensive and easy to use, and a growing share of encrypted devices and applications use unrecoverable encryption.

The world was also less dangerous in 2000. China and Russia were friendlier, al Qaeda was a distant menace, and the Islamic State of Iraq and Syria (ISIS) did not exist. The Internet itself has changed, becoming a global high speed network that is the backbone for communications and business that is routinely exploited for crime and espionage. The advent of high speed global networks led to an explosion of crime and espionage on the Internet that few expected in 2000. Public safety faces new threats. While encryption use will reduce some risks, it will increase others.

## SURVEILLANCE CONCERNS SHIFTED THE MARKET

Most encryption products include recovery mechanisms because they enable features that customers want. For example, recovery mechanisms allow users to regain access to their accounts if they forget their password, search their historical data easily, link together their devices and apps across platforms, and access their data from anywhere in the world at any time with minimal fuss.

However, in the aftermath of the Snowden leaks, concerns about U.S. companies facilitating government surveillance have grown, creating demand for unrecoverable encryption products. Consumers want assurances that their data cannot be surreptitiously accessed. Concern about American products is driven by the perception that there are inadequate constraints, little transparency, and no oversight on U.S. law enforcement and intelligence agencies. Europe is the most vocal on this subject, but other countries have similar worries. One reason China is investing billions of dollars into building its own domestic information technology (IT) industry is to avoid the perceived risk of depending on foreign products.

1. Meaning encryption products that the National Security Agency (NSA) and Federal Bureau of Investigation (FBI) did not have the ability to "break" in 2000.

To address these concerns and protect market share, some companies are adopting unrecoverable encryption that does not permit cooperation with law enforcement requests. They can tell their customers that not only is it against company policy, it is technically impossible for them to facilitate U.S. government access to the data, whether it is law enforcement seeking evidence with a warrant or an intelligence agency with a national security letter.

The most significant changes since 2000 are the growth of unrecoverable full disk encryption (where data stored on a device's disk drive is encrypted) and the availability of easily downloaded and installed end-to-end encrypted messaging applications. It is the growth of these commercial encryption products and services offering unrecoverable encryption to a mass market that is of the greatest concern to law enforcement and intelligence agencies.

For governments and consumers, there is growing unease over the use and ownership of online personal data. In the absence of more comprehensive privacy solutions, encryption offers a means for individuals to assert control over their data. There is no simple solution, however: consumers want greater control over their data, but governments cannot abandon their responsibilities for public safety and national security.

## THE ENCRYPTION DEBATE AND BACKDOORS

The encryption debate has been cast as a choice between unacceptable options that would weaken encryption by creating a "backdoor" or "golden key." These loaded terms polarize the discussion over unrecoverable encryption. The term *backdoor* implies surreptitious access and a lack of accountability. What law enforcement agencies want is the use of recoverable encryption that can permit lawful access with appropriate oversight. The problem is that mandating recoverability is costly and complex to implement. It would affect the ability of firms to sell in foreign markets. And it is unlikely to fully deliver the desired public safety benefits because criminals and terrorists could still leverage non-U.S. encryption products and open source encryption tools.

Claims that blocking unrecoverable encryption will unacceptably damage cybersecurity are also overstated. Judging from the practice of intelligence agencies and large corporations that secure classified and sensitive proprietary information using recoverable encryption, data can be kept secure while using encryption that allows for plaintext recovery.

Currently, the encryption debate is framed as a zero-sum choice between digital privacy and security on one hand and the ability of law enforcement to stop terrorists and catch child pornographers on the other. Progress is hampered by hyperbole and misinformation. A range of hypothetical solutions have been discussed, but rarely with any meaningful inquiry into the effectiveness or consequences of such solutions based on a serious, data-driven evaluation of how technology architectures or business models will be affected.

Encryption creates both benefits and costs. For this report, we sought data on encryption use and its effect on investigations, global markets, and new technologies to better understand the risks that encryption poses to public safety. While the trend toward greater use of unrecoverable

encryption suggests that the risk to public safety will increase, we could not find data that suggests this risk is unbearable. Our basic conclusion is that the benefits of mandating access to encrypted data would not outweigh the costs. Law enforcement access to encrypted data is an issue, but the magnitude of the challenge is not yet significant enough to justify decryption mandates.

02

# How Prevalent Is Unrecoverable Encryption?

As large Internet companies such as Google and Netflix adopt and promote HTTPS [hyper text transfer protocol secure], encrypted web traffic has grown to more than 50 percent of total Internet traffic in 2016.[1] But the use of HTTPS[2] or the total amount of encrypted Internet traffic is not a good measure of the challenge for law enforcement. The vast majority of encrypted Internet traffic is of no interest to law enforcement, such as encrypted streaming video for entertainment platforms like Netflix. For law enforcement investigations, e-mail, chat, voice, video communications, and file sharing are of greatest interest, but taken together these platforms account for less than 10 percent of total Internet traffic in North America.[3]

What changed the encryption landscape was when major IT companies adopted stronger encryption features in widely used consumer communications platforms that are impervious to existing law enforcement techniques and tools. Four trends have rendered traditional methods to access the content of communications and stored data more challenging for law enforcement.

First, device makers and mobile application developers have moved to adopt stronger encryption architectures that utilize *end-to-end encryption* with *perfect forward secrecy*, a cryptographic feature that generates and stores private keys on the user's device and is inaccessible to the service provider, even if the service provider is willing to assist law enforcement. Each message or communications session is encrypted with a new key that is discarded after each session to ensure that no messages sent in the past or the future can be decrypted with the same key.

Second, companies are using more robust methods to *authenticate encryption* to ensure the integrity of communications. Authentication provides assurance that both ends of the

1. Encrypted traffic comprises 50 percent to 70 percent of global internet traffic based on estimates from two sources: 70 percent—Sandvine, *2016 Global Internet Phenomena Spotlight: Encrypted Internet Traffic* (Waterloo, ONT: Sandvine, 2016), https://www.sandvine.com/trends/encryption.html; 50 percent—Comments by Parisa Tabriz, Google Security Princess, April 2016.

2. HTTPS is a network protocol that uses basic encryption.

3. Sandvine, *2016 Global Internet Phenomena Spotlight*.

communication are who they say they are. Use of temporary authentication keys and more robust authentication functions, such as forced time delays between passcode attempts or auto-erase features, make it difficult for law enforcement to access encrypted communications and stored data.

Third, communications content is increasingly *ephemeral*. Some chat and e-mail applications are moving to adopt transient messaging by automatically deleting messages from devices and servers immediately after they are viewed (e.g., Snapchat and Wickr). Ephemeral messaging platforms and data retention policies that favor minimization render data inaccessible to law enforcement, regardless of encryption. If the data, even if it is not encrypted, is deleted, it cannot be provided to law enforcement. Importantly, this affects both metadata and the content of communications.

Fourth, companies are taking steps to offer products with the above features on widely used consumer messaging platforms and are *enabling these features by default*. This significant trend means that users no longer have to manually turn on encryption. In other words, billions of users worldwide have adopted unrecoverable encryption without even knowing it as mobile messaging companies have incorporated features into their products and services that guard against eavesdropping or intercepting communications, but also prevent the companies themselves from being technically capable of accessing user data.

## END-TO-END ENCRYPTED MOBILE MESSAGING

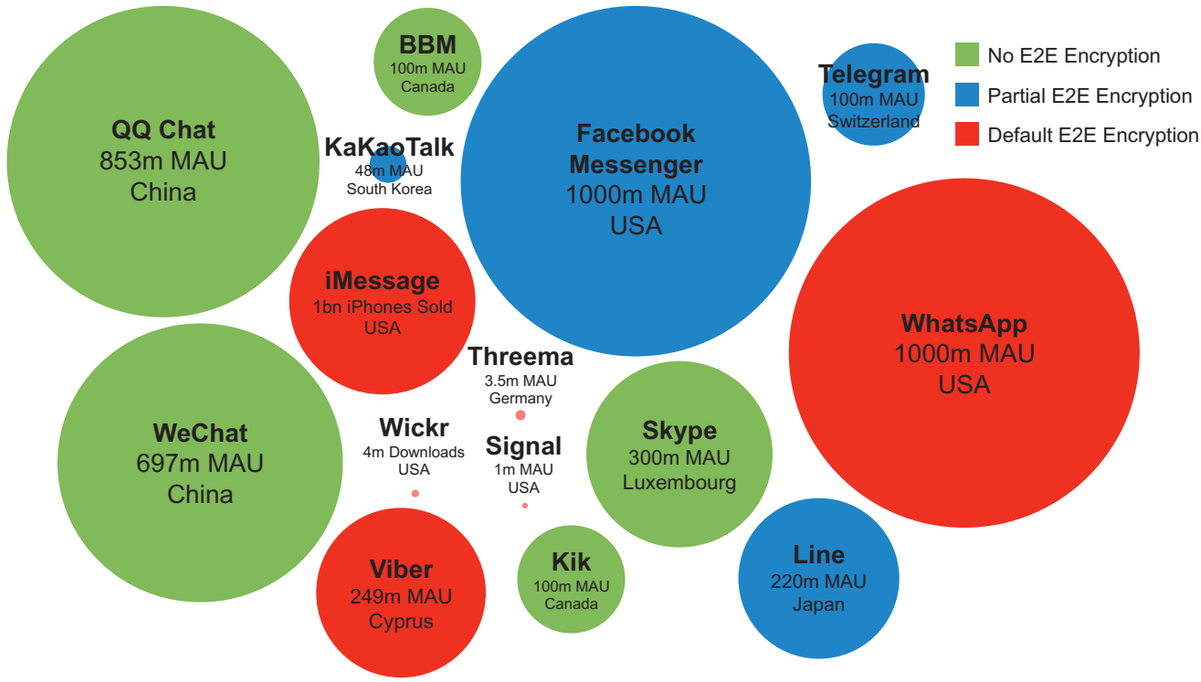
Mobile messaging applications such as WhatsApp, Facebook Messenger, iMessage, Telegram, Skype, Line, and others are rapidly becoming the dominant mode of communication around the world. Growing demand for instant messaging (IM) means that its share of global message traffic is estimated to grow from 50 percent to 63 percent in the next few years. Instant messaging traffic is expected to grow more than 20 percent annually through 2019, nearly doubling to almost 100 trillion messages per year (or almost 274 billion per day).[4] Many of these apps, called over-the-top (OTT) services and applications, have recently moved to adopt end-to-end encryption, making them inaccessible to law enforcement agencies.

Three of the world's top twelve mobile messaging apps, as measured by monthly active users (MAUs), have enabled unrecoverable end-to-end encryption by default. This means more than 1.5 billion individuals globally use end-to-end encrypted messaging applications. Many of the largest messaging platforms have adopted end-to-end encryption (E2EE) in the last year, including WhatsApp, Facebook Messenger (not by default), and Viber. The largest end-to-end encrypted messaging app by number of users is WhatsApp, which implemented E2EE by default in April 2016.[5] Less than 10 percent of Internet users in the United States use WhatsApp, but for many other countries WhatsApp is a primary mode of communication. Approximately 34 percent of global Internet users

4. Windsor Holden, "A2P Messaging," Juniper Research, September 19, 2016, https://www.juniperresearch.com/researchstore/content-applications/mobile-online-messaging/sms-rcs-im-markets.

5. Jan Koum and Brian Acton, "End-to-End Encryption," *WhatsApp Blog*, April 5, 2016, https://blog.whatsapp.com/10000618/end-to-end-encryption.

## Figure 2.1. Mobile Messaging Apps Usage




Note: E2E = end-to-end; MAU = monthly service users. Some users use multiple mobile messaging apps.
Source: Statista, "Most Popular Global Mobile Messaging Apps as of April 2016, Based on Number of Monthly Active Users (in Millions)," http://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/; Rob Price, "Germany's Most Popular Paid App Is a Secure Messenger Loved By Millions—Now It's Taking on the US," *Business Insider*, June 18, 2015, http://www.businessinsider.in/Germanys-most-popular-paid-app-is-a-secure-messenger-loved-by-millions-now-its-taking-on-the-US/articleshow/47718937.cms; Lorenzo Franceschi-Bicchierai, "You Can Now Send Self-Destructing Wickr Messages from Your Computer," December 4, 2014, http://mashable.com/2014/12/04/wickr-desktop-app/#njk0Dvt1.Eqk.

have WhatsApp on their phones. In Latin America and the Middle East about 66 percent of Internet users use WhatsApp.[6]

Juniper Research estimates that roughly 108 trillion messages were sent 2016.[7] Almost 90 percent of those messages are instant messages and e-mails, the majority of which are encrypted, often using HTTPS encryption that is accessible to law enforcement through the service provider. Based on the share of messaging platforms that employ end-to-end encryption, we estimate that about 18 percent of total communications traffic uses end-to-end encryption and inaccessible to law enforcement.

6. Statista, "Usage Penetration of WhatsApp in Selected Global Regions as of 4th Quarter 2015," http://www.statista.com/statistics/321460/whatsapp-penetration-regions/.

7. This includes SMS, multimedia message service (MMS), e-mail, IM, and social media posts. See Holden, "A2P Messaging."

The share of unrecoverable encryption as a share of total communications traffic is likely to grow, as instant messaging becomes increasingly dominant. Meanwhile, growth in e-mail and short message service (SMS) messaging, which are usually accessible to law enforcement agencies, is expected to be flat.

The rapid growth of IM means that its share of global message traffic will increase from 50 percent to 63 percent.[8] These estimates imply that even if the share of instant messages that are end-to-end encrypted remained constant, more than 22 percent of global messaging will be end-to-end encrypted and inaccessible to law enforcement by 2019 as instant messaging becomes an increasingly dominant mode of communication.

Some messaging applications present challenges for law enforcement that are unrelated to encryption. For example, Kik is a messaging platform that is known to be used by child predators, who use it to identify victims and share sexually explicit material. Kik is not end-to-end encrypted, but it does not retain most user data on its servers, making it impossible to service search warrants.[9] Telegram, a popular messaging app, supports end-to-end encryption but does not enable it by default. However, law enforcement has struggled to access even unencrypted communications over Telegram, which hosts its data in Switzerland. Telegram is popular with terrorist groups and was used by the jihadi killers of a French priest in August 2016.[10] Developed by Russian Internet entrepreneurs who were forced out of Russia and fled to Germany, Telegram refuses to comply with law enforcement requests for data.[11]

## FULL DISK ENCRYPTION

The use of unrecoverable encryption is a growing trend in the mobile space, particularly as full disk encryption (FDE) is becoming the norm for a growing share of consumer devices. Apple is the largest provider of mobile FDE in the world. Approximately 13 percent of all mobile devices globally run iOS, and more than 95 percent of all iOS devices currently run iOS 8 or higher, which Apple says even they cannot access.[12] Device encryption on Apple phones is a likely a bigger challenge for U.S. law enforcement than for other countries because 44 percent of all mobile devices in the United States run iOS.

---

8. Calculated by CSIS based on Juniper Research data: Lauren Foye, "Mobile & Online Messaging: SMS, RCS & IM Markets 2015-2019," *Juniper Research*, September 6, 2015, http://www.juniperresearch.com/researchstore/content-applications/mobile-online-messaging/sms-rcs-im-markets.

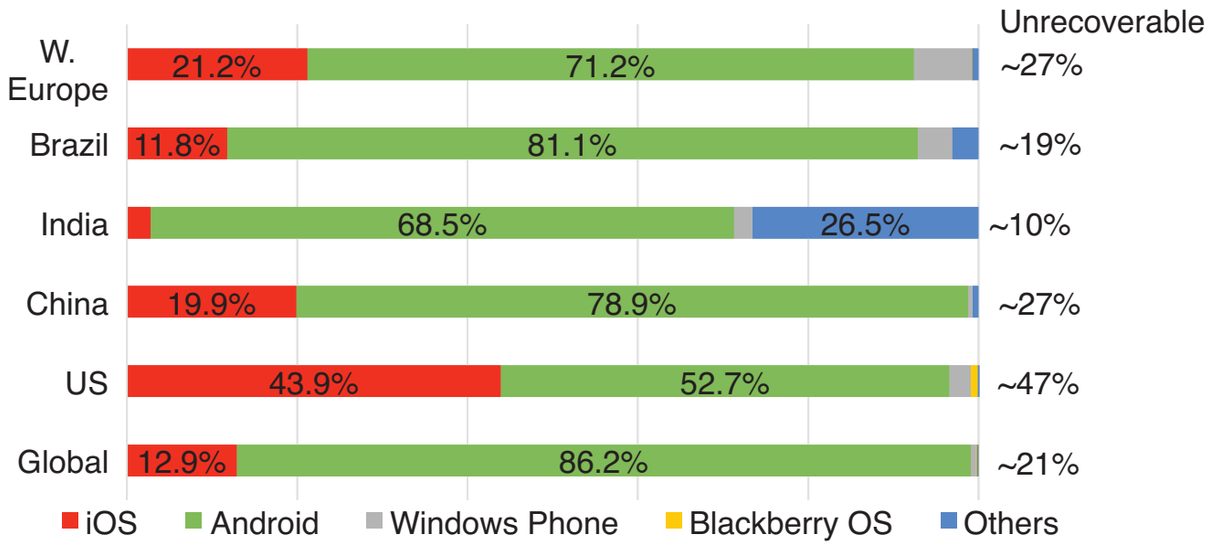
9. Department of Homeland Security Office of Intelligence and Analysis, "Going Dark—Covert Messaging Applications and Law Enforcement Implications," September 29, 2015, https://assets.documentcloud.org/documents/2500347/going-dark-covert-messaging-apps.pdf.

10. "France Terror: Girl, 16, Investigated over Telegram 'Attack Plan,'" BBC, August 10, 2016, http://www.bbc.com/news/world-europe-37033271; "TIMELINE: Aaron Driver's History of Radicalization," CBC, August 11, 2016, http://www.cbc.ca/news/canada/aaron-driver-timeline-1.3717169.

11. Electronic Frontier Foundation, "Secure Messaging Scorecard," https://www.eff.org/secure-messaging-scorecard.

12. Apple, "Apple App Store Support," April 18, 2016, https://developer.apple.com/support/app-store/.

## Figure 2.2. Market Share of Leading Smartphone Operating Systems




Note: Unrecoverable share assumes 95 percent of iOS devices and 10 percent of Android devices are protected by unrecoverable encryption.

Source: Statista, "Global Market Share Held by the Leading Smartphone Operating Systems in Sales to End Users from 1st Quarter 2009 to 4th Quarter 2015"; Statista, "Subscriber Share Held by Smartphone Operating Systems in the United States from January 2012 to February 2016"; Statista, "Market Share Held by Mobile Operating Systems in China from January 2012 to December 2015"; Statista, "Market Share Held by Mobile Operating Systems in Brazil from January 2012 to December 2015"; Statista, "Market Share Held by Mobile Operating Systems in India from January 2012 to July 2015"; Statista, "Market Share of Smartphone Unit Shipments in Western Europe in 2013 and 2014, by Operating System."

Google's Android is the largest mobile operating system in the world, making up more than 86 percent of the global mobile market. Currently, less than 10 percent of Android devices have enabled FDE, partly because the Android mobile industry is not vertically integrated. Although the operating system is developed by a single company (Google), there is a relatively large number of device makers, which means that the Android ecosystem is less coordinated than Apple's system.[13] Android is also more popular in countries like China and India where the average consumer is more price sensitive and thus more likely to purchase less powerful mobile devices that do not have enough processing power to support FDE without compromising user experience.

Because about 47 percent of all mobile devices in the United States have FDE (the global average is 21 percent), FDE on mobile devices likely poses a larger problem for U.S. law enforcement than it does for other countries. This could change dramatically if all iOS and Android devices adopt FDE

13. Jack Nicas, "Google Faces Challenges in Encrypting Android Phones," *Wall Street Journal*, March 14, 2016, http://www.wsj.com/articles/google-faces-challenges-in-encrypting-android-phones-1457999906#:q2ds8BIEH6PAKA.

as their default, resulting in the majority of data stored on smartphones becoming inaccessible to law enforcement in all countries.[14]

## E-MAIL ENCRYPTION

In contrast to mobile messaging apps, end-to-end encrypted e-mail is not widely used by consumers or enterprises and is unlikely to be widely adopted, largely for business reasons. E-mail users have different expectations than instant messaging users. They expect to be able to access stored e-mails, recover account passwords if they forget them, access their e-mail from any device, and send e-mails to their friends using different e-mail platforms. End-to-end encryption renders all of these functions difficult or impossible.

Moreover, most e-mail services are free, and providers monetize the service by mining user data, including the content of e-mails. None of the major consumer e-mail providers have deployed end-to-end encryption. The largest e-mail providers globally, with hundreds of millions of users, have adopted secure socket layer (SSL)/transport layer security (TLS) encryption, but none of them use end-to-end encryption that is unrecoverable by law enforcement. By comparison, end-to-end encrypted e-mail providers such as ProtonMail and Tutanota are tiny, with just 1 million users each.[15] But growth of end-to-end encrypted e-mail is rising dramatically in the aftermath of recent large-scale e-mail hacks, such as the intrusions into the Democratic National Committee and Yahoo.[16]

---

14. Statista, "Global Market Share Held by the Leading Smartphone Operating Systems in Sales to End Users from 1st Quarter 2009 to 4th Quarter 2015," http://www.statista.com/statistics/266136/global-market-share-held-by-smartphone-operating-systems/; Statista, "Subscriber Share Held by Smartphone Operating Systems in the United States from January 2012 to February 2016," http://www.statista.com/statistics/266572/market-share-held-by-smartphone-platforms-in-the-united-states/; Statista, "Market Share Held by Mobile Operating Systems in China from January 2012 to December 2015," http://www.statista.com/statistics/262176/market-share-held-by-mobile-operating-systems-in-china/; Statista, "Market Share Held by Mobile Operating Systems in Brazil from January 2012 to December 2015," http://www.statista.com/statistics/262167/market-share-held-by-mobile-operating-systems-in-brazil/; Statista, "Market Share Held by Mobile Operating Systems in India from January 2012 to July 2015," http://www.statista.com/statistics/262157/market-share-held-by-mobile-operating-systems-in-india/; Statista, "Market Share of Smartphone Unit Shipments in Western Europe in 2013 and 2014, by Operating System," http://www.statista.com/statistics/398684/western-europe-smartphone-shipments-operating-systems-share/.

15. Henning Steier, "Protonmail Ende Januar offen für alle," *Neue Bürcher Beitung*, December 16, 2015, http://www.nzz.ch/digital/protonmail-ende-januar-offen-fuer-alle-ld.3685; Waqas, "Encrypted Email Startup Tutanota Reaches 1 Million Users," *Hackread.com*, February 24, 2016, https://www.hackread.com/encrypted-email-startup-tutanota-reaches-1-million-users/.

16. Paul Sawers, "Encrypted Email App ProtonMail Reports Surge in Users after Latest Yahoo Hack Revealed," *Venturebeat.com*, December 22, 2016, http://venturebeat.com/2016/12/22/encrypted-email-app-protonmail-reports-surge-in-users-after-latest-yahoo-hack-revealed/.

## ENTERPRISE ENCRYPTION

Many of the largest encryption customers are enterprises, which use encryption to protect intellectual property and communications and secure their data against cyber attacks. The majority of enterprises use recoverable encryption because it is in their interest to do so. For a business, unrecoverable encryption can lead to the loss of essential data and intellectual property if passwords are lost or employee turnover occurs. It can also raise liability and regulatory risks if employees use it to mask illegal or unethical activity. As a result, major enterprise encryption providers include recovery solutions and key management systems in their products and services.

Bring your own device (BYOD) policies, in which companies allow employees to use their personal mobile devices (which are increasingly protected by unrecoverable encryption by default) for work, raise additional issues. As employers move to BYOD as a normal business practice, they may require employees to use specific applications for business or install remote access applications on their personal devices to ensure that they can monitor and protect company information on those devices.

## VIRTUAL PRIVATE NETWORKS AND ANONYMIZED BROWSERS

Anonymized web browsers like Tor present challenges to law enforcement, but they are not widely used. Virtual private networks (VPNs), which use encryption to provide a secure connection that is difficult to monitor, are more common. One study found that globally one in four Internet users has used a VPN. Roughly 18 percent of global Internet users use a VPN at least once a week, and about 6 percent use one every day.[17] VPNs can slow browser speeds or prevent users from accessing some websites. It also prevents web-based services from customizing their offerings for specific users. As a result, consumer VPN use is most common in countries where users are concerned about censorship and government surveillance, while Western democracies see much lower rates of use. For example, VPN use in China was almost double the U.S. rate in 2015.[18]

17. Katie Young, "1 in 4 VPN Users Accessing Daily," Global Web Index, February 17, 2016, http://www.globalwebindex.net/blog/1-in-4-vpn-users-accessing-daily.

18. Statista, "When You Access the Internet, Do You Do So Using a VPN or Proxy Server?," Q4 2015, http://www.statista.com/statistics/301204/top-markets-vpn-proxy-usage/.

# 03

# Data on Going Dark

The data that is available on the effect of encryption on law enforcement is limited. Senior law enforcement officials have referred to incidents where encryption presented a challenge, but have not provided a comprehensive picture.[1] There is some information, however, on cases where law enforcement has attempted to access data, such as through Title III wiretaps and device seizures, and were thwarted by unrecoverable encryption. This may not represent the full scope of the challenges faced by law enforcement, but it presents a starting point for understanding the effect of encryption use.

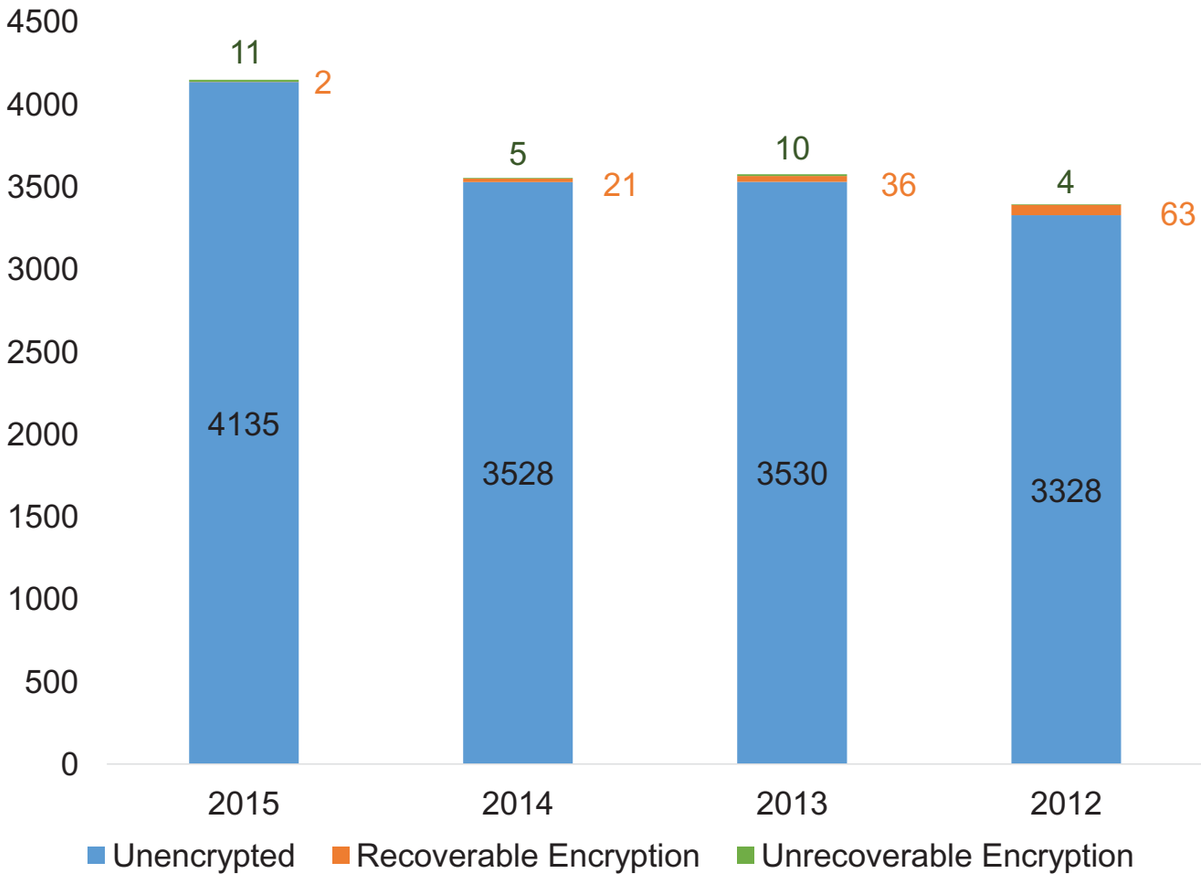
## ENCRYPTION AND TITLE III WIRETAPS

Data on the effect of encryption on Title III wiretaps suggests that encryption has not significantly hampered law enforcement investigations. Title III wiretaps are used for real-time surveillance of communications in motion. To execute a wiretap, investigators must demonstrate probable cause to obtain a warrant and seek assistance from service providers covered by the Communications Assistance for Law Enforcement Act (CALEA)[2] to execute the intercept. According to annual Title III wiretap reports compiled by the U.S. Court System, a very small share of Title III wiretaps encounter encryption, and the majority of those are ultimately decrypted.

The first time that unrecoverable encryption was reported in a Title III wiretap was in 2012. That year, 67 wiretaps encountered encryption, of which four were unrecoverable. From 2012–2015, 152 Title III wiretaps encountered encryption, of which 30 were unrecoverable. During this period

1. Dan Froomkin and Natasha Vargas-Cooper, "The FBI Director's Evidence against Encryption Is Pathetic," *Intercept*, October 17, 2014, https://theintercept.com/2014/10/17/draft-two-cases-cited-fbi-dude-dumb-dumb/.
2. See appendix B for additional information on CALEA.

**Figure 3.1. Federal and State Title III Wiretaps**




Source: U.S. Courts, "Wiretap Reports," accessed September 30, 2016. http://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports.

more than 14,500 wiretaps were ordered, meaning that just 0.2 percent of wiretaps encountered unrecoverable encryption.[3]

Law enforcement officials argue that this statistic is misleading. Title III wiretap applications are complex and time consuming. Investigators know what apps are unrecoverable, so they often do not even bother to request wiretaps in cases where such apps are being used by suspects. Instead, they pursue other investigative techniques to get the evidence needed for prosecution.

## ENCRYPTED MOBILE DEVICES SEIZED BY LAW ENFORCEMENT

Comprehensive statistics on encryption as an obstacle to law enforcement are currently unavailable, but based on available data, full disk encryption on mobile devices poses a greater challenge.

3. U.S. Courts, "Wiretap Reports," accessed September 30, 2016, http://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports.

In April 2016, Amy Hess, executive assistant director of the FBI's Science and Technology Branch, testified that about 30 percent of the more than 3,000 mobile phones that the FBI seized in the previous six months were password protected, and in about 13 percent of those cases the FBI was unable to access any data on those phones, which is about 120 phones.[4] She also said that she expects that number to continue to grow as unrecoverable encryption is deployed on more devices.

State and local law enforcement are also affected. For example, the Los Angeles Police Department and Los Angeles County Sheriff had a total of 450 inaccessible phones in evidence as of the end of February 2016, while the New York County District Attorney's office seized 423 inaccessible phones between October 2014 and October 2016.[5] The 423 inaccessible phones seized by the New York County District Attorney's office represent approximately 34 percent of the total phones seized by that office over the same period, and relate to a range of cases including murders, sex crimes, and complex financial crimes.[6]

## USE OF UNRECOVERABLE ENCRYPTION BY MALICIOUS ACTORS

Islamic extremists are using unrecoverable encryption to attempt to evade law enforcement and intelligence agencies, with ISIS providing instructions for their followers on how to use encryption in recruiting and coordinating operations. Abdelhamid Abaaoud, the European ISIS leader who directed the terrorist attacks on Paris in November 2015, included computer security in his training for his operatives, teaching them to use open source TrueCrypt disk encryption software to hide data on their computers from law enforcement.[7] Al Qaeda's media arm even produced its own encrypted communications app, Amn al-Mujahid, to allow its members to communicate.[8]

However, most terrorists do not appear to rely on encryption for their operational communications. They evade surveillance using a number of alternative means. The Paris attackers, for example, used burner phones[9] and other means (such as couriers or prearranged code words) to evade surveillance. Terrorist groups use encryption, but we found no evidence that this is their

4. Erin Kelly, "FBI Can't Unlock 13% of Password-Protected Phones It Seized, Official Says," *USA Today*, April 19, 2016, http://www.usatoday.com/story/news/politics/2016/04/19/fbi-cant-unlock-13-password-protected-phones-seized-official-says/83224860/.

5. Manhattan District Attorney's Office, "Smartphone Encryption and Public Safety: An Update to the November 2015 Report," November 2016, http://manhattanda.org/sites/default/files/Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety:%20An%20Update.pdf.

6. Ibid.

7. Rukmini Callimachi, "How ISIS Built the Machinery of Terror under Europe's Gaze," *New York Times*, March 29, 2016, http://www.nytimes.com/2016/03/29/world/europe/isis-attacks-paris-brussels.html?_r=0.

8. Site Intelligence Group, "Al-Fajr Media Center Releases New Encryption Program, 'Amn Al-Mujahid,'" December 10, 2013, https://ent.siteintelgroup.com/Software-and-Technical-Materials/al-fajr-media-center-releases-new-encryption-program-amn-al-mujahid.html.

9. Rukmini Callimachi, Alissa J. Rubin, and Laure Fourquet, "A View of ISIS's Evolution in New Details of Paris Attacks," *New York Times*, March 19, 2016, http://www.nytimes.com/2016/03/20/world/europe/a-view-of-isiss-evolution-in-new-details-of-paris-attacks.html?ref=world&_r=1&mtrref=www.nytimes.com.

## Figure 3.2. "Warrant-Proof" Devices Seized by Local Law Enforcement

| Agency | Devices | Time Period |
|---|---|---|
| New York County DA (Manhattan) | 423 | Oct 2014 - Oct 2016 |
| Los Angeles Police | 300 | Total in evidence |
| Charlotte-Mecklenburg Police Department | 160 | Total in evidence |
| Suffolk County DA (Boston) | 151 | Total in evidence |
| Los Angeles County Sheriff | 150 | As of Feb 28, 2016 |
| Austin Police Department | 45 | Total in evidence |
| Chicago Regional Computer Forensic Laboratory | 30 | 1H 2016 |

Note: DA=District Attorney.

primary means of securing their communications, because they either avoid the use of Western communications technology or use communications techniques to evade surveillance that do not rely on encryption. We examined publicly available material on six major terrorist attacks—Mumbai, London, Boston, San Bernardino, Paris, and Brussels—plus several failed attempts (New York and Koln) and data taken from devices recovered in the conflicts in the Middle East. In no instance did we find evidence that encryption played a determinative role in these incidents. The attackers relied on surprise and responder confusion to achieve success.[10]

While online recruitment by terrorist groups is a major concern, encryption also does not appear to play a major role in this. In some instances (e.g., London, Brussels), propinquity better explains recruitment—the attackers all lived in the same neighborhoods and had similar social backgrounds. In other cases, terrorists used a combination of false identities and multiple website and chatroom addresses to attempt to evade surveillance. When a site is forced to move, informal networks based on chatrooms or e-mail inform potential recruits of the new network address. This word-of-mouth system to distribute new addresses is very effective. The ability to use social networks for recruitment does not rely on encryption.

## CRIMINAL USE

To get an accurate sense of how unrecoverable encryption affects security and public safety, we need to look at the net effect. Being able to obscure data and communication has both positive and

10. Robert Graham, "How Terrorists Use Encryption," *CTC Sentinel* 9, no. 6 (June 2016): 20–25, https://www.ctc.usma.edu/posts/how-terrorists-use-encryption; Cyberkov, "ISIS OPSEC Guide," as cited in Kim Zetter, "Security Manual Reveals the OPSEC Advice ISIS Gives Recruits," *Wired*, November 2015, http://www.wired.com/wp-content/uploads/2015/11/ISIS-OPSEC-Guide.pdf; Callimachi et al., "A View of ISIS's Evolution"; Glyn Moody, "Paris Terrorists Used Burner Phones, Not Encryption, to Evade Detection," *ArsTechnica*, March 21, 2016, http://arstechnica.com/tech-policy/2016/03/paris-terrorist-attacks-burner-phones-not-encryption/.

negative results. The benefits accrue in cybersecurity and privacy. The costs accrue in decreased surveillance capabilities, affecting law enforcement and counterterrorism. Communications surveillance and lawful access to communications are invaluable tools in deterring and prosecuting crime and in counterterrorism. What is not clear is how much the current use of unrecoverable encryption actually degrades these capabilities and whether there is any concomitant increase in criminal activity.

Child pornography, which was almost eradicated in the 1980s, has rebounded because the Internet made it easier to engage in this behavior, increasing an incredible 15 times (by the number of cases) between 1995 and 2006.[11] This increase occurred well before the advent of widely available unrecoverable encryption. The principal cause of the increase is access to the Internet making this easier to share. The effect of encryption, however, complicates efforts to identify and prosecute those who engage in child pornography.

Drug traffickers have used encryption to evade surveillance for years. The Zeta organization of Mexico even built its own mobile, encrypted, communications network a decade ago.[12] Encrypted apps provide a cheap alternative to proprietary networks. Drug traffickers used encrypted messaging app Surespot to evade law enforcement as early as 2014.[13] Guadalajara cartel boss Rafael Caro Quintero used WhatsApp video messages to communicate with other cartel leaders,[14] while Sinaloa cartel boss Joaquin "Chapo" Guzman attempted to use a Blackberry to secure his messages while in hiding. The use of encryption changes the nature and complexity of antidrug operations, but as one political official put it: "Drug dealers are using encrypted devices, money launderers are using encrypted devices but they are still being caught, we are still making arrests."[15]

There are many troubling examples, but judging from the available data, the number of cases affected by encryption is small, ranging from a few dozen to several hundred, varying from jurisdiction to jurisdiction. What the FBI and other law enforcement agencies are worried about is a potential future where large technology companies will provide unrecoverable encryption by default for a growing share of communications platforms.

---

11. U.S. Department of Justice, "Child Pornography," updated June 3, 2015, https://www.justice.gov/criminal-ceos/child-pornography; Tracey Harrington McCoy, "The Sexual Predator App with a 100 Percent Conviction Rate," *Newsweek*, August 18, 2014, http://www.newsweek.com/2014/08/29/sexual-predator-app-100-percent-conviction-rate-264947.html; Mark Motivans and Tracey Kychelhahn, "Federal Prosecution of Child Sex Exploitation Offenders, 2006," *Bureau of Justice Statistics Bulletin*, December 2007, http://www.bjs.gov/content/pub/pdf/fpcseo06.pdf; Jérôme Endrass et al., "The Consumption of Internet Child Pornography and Violent and Sex Offending," *BMC Psychiatry* 9 (July 2009), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2716325/pdf/1471-244X-9-43.

12. Michael Weissenstein, "Mexico's Cartels Build Own National Radio System," Yahoo! News, December 27, 2011, https://www.yahoo.com/news/mexicos-cartels-build-own-national-radio-system-200251816.html?ref=gs; Patrick Howell O'Neill, "How a Drug Cartel Used Encryption and a Fake Website to Launder Millions," *Daily Dot*, October 17, 2016, http://www.dailydot.com/layer8/mexican-cartel-encryption/.

13. Department of Homeland Security Office of Intelligence and Analysis, "Going Dark—Covert Messaging Applications and Law Enforcement Implications," September 29, 2015, https://assets.documentcloud.org/documents/2500347/going-dark-covert-messaging-apps.pdf.

14. Ibid.

15. Nick Ralston, "Are Encrypted Phones Allowing Criminals to Get Away with Murder?," *Sydney Morning Herald*, May 24, 2015, http://www.smh.com.au/nsw/are-encrypted-phones-allowing-criminals-to-get-away-with-murder-20150523-gh82gv.html.

The use of encryption is a subset of a larger problem created by the Internet. In addition to its immensely positive contributions to societies, the Internet also makes it easier to engage in illicit behavior, a trend exacerbated by both the transborder nature of Internet activities and the absence of enforceable legal constraints on online behavior. Malicious actors' use of encryption is an outgrowth of this larger problem, not its cause. For now, the most likely effect of greater use of unrecoverable encryption is to make prosecution of criminals more onerous. It likely does not mean an increase in the number of people engaging in the criminal activity. Alternative sources of digital evidence are available, such as metadata or unencrypted video, audio, and other types of data increasingly available with the expansion of the so-called Internet of Things. But the rules and policy around leveraging these new data sources are unclear and law enforcement lacks the technical expertise for collection and analysis of this data.

## SURVEILLANCE AND ENCRYPTION

In many ways, the debate is about surveillance. Societies need to weigh the risk that encryption restrictions could pose to privacy (and, perhaps, to sales in the global market) against the potential risks to public safety and security from decreased surveillance. Alternate investigative techniques using metadata and advanced data analytics could compensate, to a degree, for greater encryption use by allowing agencies to identify potential terrorists or criminals. This alternative is cumbersome and unsatisfactory in many ways, but our assessment is that while greater use of encryption makes digital surveillance less efficient, it does not render it ineffective.

Since precise metrics on risk and effect do not exist for encryption, we are often left with conflicting opinions. Those who must manage the risk of crime or terrorism fear the rate of increase in unrecoverable encryption use creates unacceptable risk; those who fear surveillance argue that any restriction on encryption is the real source of risk. Better policymaking requires better data, including monitoring the rate of change in the number of investigations and prosecutions thwarted by encryption and the role of encryption in terrorist operations.

04

# Global Concern, but No Global Consensus

One shortcoming of the U.S. encryption debate is its overwhelmingly American focus. Encryption is not just an American issue. Several other countries favor limits on the use of unrecoverable encryption and have moved to block its use. Sometimes this involves laws and regulations, while other times it involves secret agreements between governments and companies. In other cases, there are legal requirements that service providers design and operate their systems in a way that allows them to decrypt data for the government.

More than half of the world's Internet users live in countries with laws that allow them to mandate some sort of decryption assistance from companies or individual users. Most people live in countries where encryption use is restricted in some way, although how these restrictions are enforced varies widely. To assess global attitudes toward encryption, we looked at 15 countries that account for more than 60 percent of global Internet users. Of these 15 countries, 7 (who are home to roughly half of the world's internet users) have laws that allow them to require encryption providers to maintain the capability to decrypt data. The other 8 countries are smaller, accounting for about 16.6 percent of global Internet users, and many of these countries, while not requiring recoverability, use other policies to manage encryption.

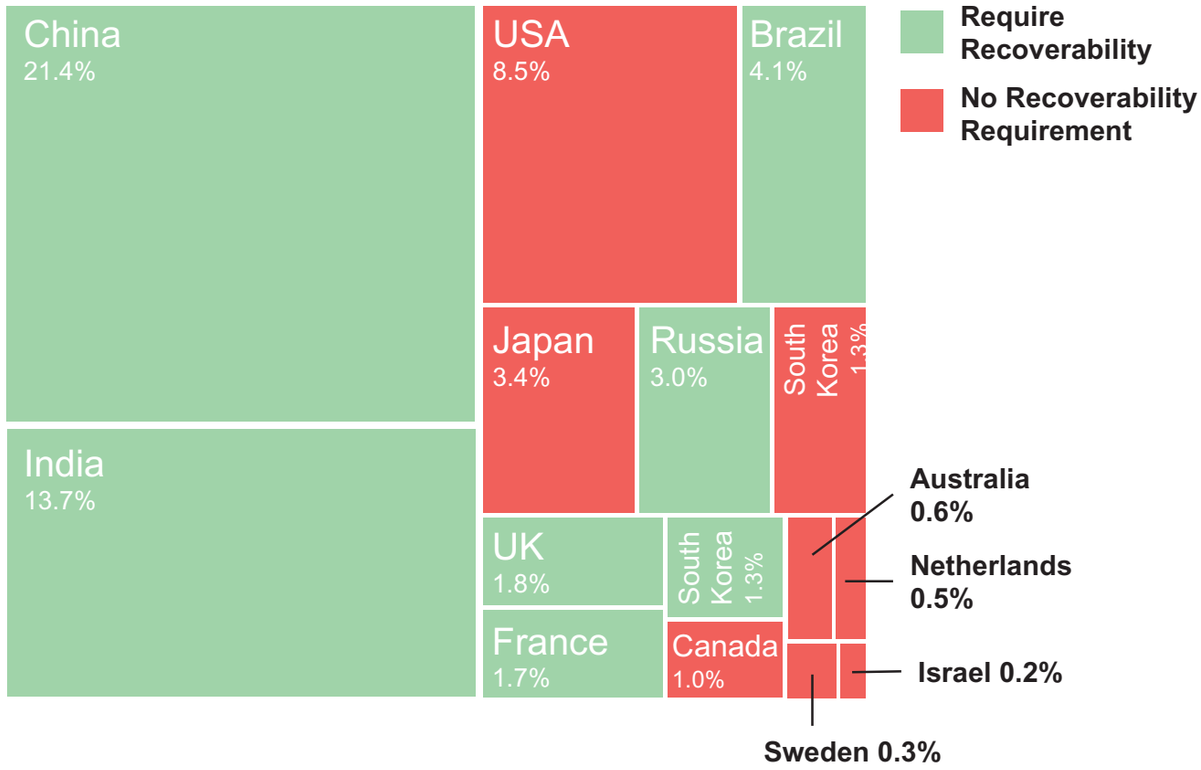
A survey of global encryption products found 846 encryption products, 546 of which are produced outside the United States.[1] Almost half of these products were made in countries that require encryption providers to maintain the ability to provide access.

## COUNTRIES WITH LAWS REQUIRING RECOVERABILITY

China and Russia have multiple laws governing access to encrypted data. Both countries have had encryption licensing regimes since the late 1990s that require encryption providers to submit

1. Bruce Schneier, "Worldwide Encryption Products Survey," Schneier on Security (blog), February 11, 2016, https://www.schneier.com/blog/archives/2016/02/worldwide_encry.html.

## Figure 4.1. Share of Global Internet Users in Select Countries and Recoverable Encryption Requirements




Note: UK=United Kingdom.

Source: Internet Users Data from "Internet Users by Country," Internet Live Stats, http://www.internetlivestats.com/internet-users-by-country/; Encryption policy data based on research by CSIS team.

products and services for evaluation, and their national security services have the authority to order companies to install hardware and software in their systems to facilitate government surveillance.[2] Both countries also recently passed sweeping antiterrorism laws, which included penalties for service providers that fail to decrypt communications for the government.[3] The authoritarian approach to governance in China and Russia gives them some advantage over other countries in obtaining the data they want from domestic vendors and service providers. The new Russian

2. Article 15 of the FSB (the FSB, or Federal'naya Sluzhba Bezopasnosti, is the Federal Security Service of the Russian Federation) law states that anyone providing "electronic communications services of all types . . . shall be under obligation, at the request of federal security service organs, to include in the apparatus additional hardware and software and create other conditions required by federal security service organs to implement operational/technical measures." See European Commission for Democracy Through Law, "Federal Law of the Federal Security Service of the Russian Federation," February 24, 2012, http://www.icla.up.ac.za/images/un/use-of-force/eastern-europe/Russia/Federal%20Law%20on%20Federal%20Security%20Service%20Russia%201995.pdf; and Christopher T. Cloutier and Jane Y. Cohen, "Casting a Wide Net: China's Encryption Restrictions," King & Spalding LLC, November 11, 2011, http://www.kslaw.com/imageserver/KSPublic/library/publication/2011articles/11-11WorldECRCloutierCohen.pdf.

3. Patrick Howell O'Neill, "Russia Lawmakers Pass Sweeping Spying Law That Requires Encryption Backdoors, Call Surveillance," *Daily Dot*, June 24, 2016, http://www.dailydot.com/layer8/encryption-backdoor-russia-fsb-bill-passes/.

counterterrorism law, passed on June 24, 2016, added more explicit requirements on Internet service providers (ISPs) requiring them to provide backdoor access to their encryption and store all consumer communications for at least six months.

China has taken a number of steps that likely improve its ability to access plaintext without the cooperation or knowledge of service providers. China requires many companies to store data in China (physical access can provide advantages in gaining access to data). The Chinese government controls its national telecom service providers (providing easy access to traffic). It imposes encryption design mandates on some IT products, and may have used espionage techniques to gain access to data and passwords. China has also passed a counterterrorism law that requires telecom operators and "enterprises providing encrypted transmission services" to "install technical interfaces" and "report cryptography schemes" to the government. Its new cybersecurity law, passed in November 2016, also requires companies to provide technical support to government agencies conducting investigations. American companies that wish to do business in China will find increasing constraints on the encryption services they can offer.[4] China is also pursuing an industrial strategy to develop national products that will compete with (and perhaps replace) foreign IT products.

In France, encryption providers are required to enter into agreements with the government to facilitate access to data they encrypt or face fines, and the prime minister's office can ban encryption services that fail to meet their legal obligations.[5] U.K. law has two key provisions for access. The first allows the home secretary to issue orders to communications providers to maintain the capability to facilitate intercepts, while the second allows decryption orders that require anyone in possession of encrypted data and the keys needed to decrypt that data to facilitate decryption for law enforcement.[6] The Investigatory Powers Bill, passed into law in late November 2016, reinforces many existing surveillance authorities, but may allow companies to contest an order to maintain the capability to decrypt communications if it is unreasonably costly or technically infeasible.[7] The scope of implementation and enforcement of these laws varies. France and the United Kingdom both allow iPhone users to access end-to-end encrypted messaging apps like WhatsApp and Viber. Brazil has had high-profile battles over encryption as part of its larger investigation into corruption among senior government officials, attempting to force WhatsApp to facilitate decryption by shutting down its service in the country and jailing its executives.[8] WhatsApp was unable to facilitate access to customer communications in response to a court order. WhatsApp remains the most popular messaging app in the country, used by more than 100 million Brazilians, or more

4. China Law Translate, "Counter-Terrorism Law (Initial Draft)," November 8, 2014, http://chinalawtranslate.com/ctldraft/?lang=en; Stewart Baker, "Deposing Tim Cook," *Washington Post*, February 25, 2016, https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/02/25/deposing-tim-cook/.

5. Legi Mobile, "Obligations des Operateurs et des Prestataires de Service," October 3, 2015, http://legimobile.fr/fr/lr/code/securite_interieure/20151003/#sec30937374.

6. Regulation of Investigatory Powers Act 2000 (chapter 23, part III), The Stationery Office Limited, September 12, 2016, http://www.legislation.gov.uk/ukpga/2000/23/part/III/data.pdf.

7. Jeremy Kahn, "U.K. Commons Passes Controversial 'Snooper's Charter' Bill," Bloomberg, June 8, 2016, http://www.bloomberg.com/news/articles/2016-06-08/u-k-commons-passes-controversial-snooper-s-charter-bill.

8. James Titcomb, "WhatsApp Shutdown in Brazil Blocks 100 Million Users," *Telegraph*, May 3, 2016, http://www.telegraph.co.uk/technology/2016/05/03/whatsapp-shutdown-in-brazil-blocks-100-million-users/.

than 50 percent of the population. The app is popular with smartphone users in many developing countries because it provides a free messaging service.

India has had some of the most sweeping powers to govern encryption in the world on the books since 2000, including mandates for both users and service providers to maintain the capability to decrypt or face prison, as well as the authority to prescribe specific implementations of encryption. However, these laws are not implemented. When the Indian government issued proposed rules to implement the policy in 2015, the rules met with fierce opposition and were retracted in a matter of days.[9]

## ENCRYPTION POLICIES IN COUNTRIES THAT DO NOT MANDATE RECOVERABILITY

Some countries that do not mandate recoverability have other policies governing the use of encryption that address law enforcement concerns. One of the most common is key disclosure mandates, where individuals holding the keys to encrypted data can be compelled to turn them over or to decrypt data. In Australia, these orders can only be served on the owner of the device or data in question, not on a service provider, and only under certain conditions. In the Netherlands service providers can be ordered to provide assistance in decrypting communications for law enforcement if they have the means to do so, but not users or suspects.

Despite not having an explicit key disclosure law or recoverability mandate, Canada appears to have a close relationship with domestic service providers, who may have provided decryption keys to the Royal Canadian Mounted Police (and perhaps other governments, such as India).[10] Israel's approach to encryption is opaque, largely centered around an encryption licensing regime run by the Ministry of Defense. Israel's laws grant broad powers to the government to regulate encryption and to enter into classified agreements with service providers to facilitate surveillance and law enforcement.[11]

In August 2016, the interior ministers of France and Germany announced a joint proposal on European internal security.[12] One of its provisions calls for the European Commission to study the possibility of issuing a directive on the rights and obligations of communications providers, including possible obligations to remove terrorist content and decrypt messages for investigations.[13] The

9. "Govt to Withdraw Controversial Draft Encryption Policy after Backlash," *Business Standard*, September 22, 2015, http://www.business-standard.com/article/current-affairs/govt-to-withdraw-controversial-draft-encryption-policy-after-backlash-115092200435_1.html.

10. Jordan Pearson and Justin Ling, "Exclusive: How Canadian Police Intercept and Read Encrypted BlackBerry Messages," Motherboard, April 14, 2016, http://motherboard.vice.com/read/rcmp-blackberry-project-clemenza-global-encryption-key-canada.

11. Matthew Waxman and Doron Hindin, "How Does Israel Regulate Encryption?," *Lawfare* (blog), November 30, 2015, https://www.lawfareblog.com/how-does-israel-regulate-encryption#.

12. Ministry of the Interior of France, "Initiative franco-allemande sur la sécurité intérieure en Europe," August 23, 2016, http://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Initiative-franco-allemande-sur-la-securite-interieure-en-Europe.

13. Ibid.

fate of this proposal is uncertain, given long standing German ambivalence on encryption restrictions (reflecting Germany's deep concern for privacy protections).

## NATIONAL APPROACHES TO ENCRYPTION CAN BE INEFFECTIVE

The Internet is a global system where individuals can acquire devices, platforms, and applications across national borders. Jurisdiction may be the greatest impediment to establishing a working encryption policy. Apart from a few countries, decryption mandates are rarely enforced in large part because users can access foreign products and services that are outside of the legal jurisdiction of their country, or they can install open source encryption tools. In other cases, governments lack the will to enforce decryption mandates due to political and economic interests.

For encryption policy to work, it must be designed for a global system and agreed upon internationally. A sustainable encryption policy needs to be perceived as legitimate globally. Countries must agree to the conditions under which a government can access plaintext, what transparency and oversight regimes are necessary, and what requirements should be imposed on vendors and service providers. A step is to establish multilateral understandings, but a global agreement may be infeasible because some countries would prefer limits on encryption. There is no consensus on which directions to take.

Absent U.S. leadership, international agreement on encryption is unlikely to emerge. The European Union could impose regulations, but it remains to be seen whether Germany will support mandates. Russia and China lack the international legitimacy to create a regime given their human rights records. India and Brazil are not sufficiently prepared to lead an international effort. In these circumstances, global encryption policies will remain uneven and reactive.

In the near term, reforming the Mutual Legal Assistance Treaty (MLAT) process would alleviate some of the challenges of cross-border requests for data. Under the current system, routine requests for digital records can take 15 to 18 months.[14] The United States is currently the largest recipient of such requests for assistance through the Department of Justice's Office of International Affairs (OIA), but staffing and resources for OIA has not kept pace with the rapid growth of requests for digital evidence.[15] Foreign governments requesting digital evidence held in the United States must also establish probable cause in order to access the content of communications, which further contributes to delays and complications. These delays in providing foreign authorities the evidence to prosecute crime and terrorism in their countries threatens reciprocal cooperation when U.S. authorities make cross-border requests for evidence for their own cases.

14. Assistant Attorney General Leslie R. Caldwell, "Remarks Highlighting Cybercrime Enforcement," Center for Strategic and International Studies, December 7, 2016, https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-highlighting-cybercrime.

15. U.S. Department of Justice Criminal Division, FY2017 Congressional Budget Submission, https://www.justice.gov/jmd/file/820926/download.

05

# Accessing Plaintext

Describing some of the ways to gain access to the plaintext of encrypted messages can help illustrate the challenges for encryption policy. There are important distinctions between mobile devices, software applications, hardware implementations of encryption, and different Internet architectures that affect the ability to gain access to plaintext. The amount of time and money required to gain access to plaintext can vary widely depending on how the encryption is implemented, whether data can be accessed physically or remotely, user practices, and other factors. In many cases, these conditions create insurmountable barriers to decryption.

"Brute force" attacks, which involve repeated efforts to guess keys or passwords, are generally ineffective against strong, well-implemented encryption products. A resource intensive approach is to attack the encryption program itself (sometimes called a cryptanalytic attack) to extract the secret key or passcode. There are several ways to do this depending on the type of information that is available to the cryptanalyst. A government agency could develop an extensive library of reverse engineered or broken encryption products, link this library to massive computing power, and then run an encrypted message through these computers to extract the key. More sophisticated programs might perform some decryption services automatically, and the encrypted traffic could be correlated with metadata[1] gained from other sources. Cryptanalytic approaches to decryption are too expensive and time consuming for a law enforcement agency to duplicate.

Devices and applications can be reverse engineered. If the product is commercially available, attackers can buy it to gain access to the internal electronics, or bombard the application with invalid commands to see how and when it fails. They can attempt to decompile software, a process that can produce the source code. Developers make coding errors. Identifying and exploiting these errors facilitates decryption, but this requires a high degree of programming expertise.

Law enforcement can access plaintext by exploiting these vulnerabilities in software and devices and implanting surveillance software on the target device or system. Surveillance tools can also be

1. Metadata is data that provides information about other data (e.g., the phone number on a phone bill).

delivered by other vehicles, such as through phishing e-mails or by corrupting the software patching process. Exploiting remote access tools commonly used by system administrators can also serve as a backdoor that can provide access to passwords, record keystrokes, or copy what appears on the screen of the target device.

The ability of an attacker to gain access to source code increases the chance of being able to decrypt. The Chinese government recently passed a set of laws that enable it to require companies to disclose their source code, store data on Chinese territory, and, in some cases, mandate the installation of government-approved encryption. These steps facilitate access to encrypted messages, particularly as they are transmitted over government-controlled telecommunication networks. Interfering in some way with the production process, either with or without the manufacturer's cooperation, makes decryption easier.

Almost all governments have the ability to monitor domestic communications. This monitoring provides access to traffic, which can allow an attacker to look for patterns that indicate who is using encryption and collate and correlate massive amounts of message traffic to provide useful data to assist in decryption. The act of sending a message itself creates data for billing and address purposes. This metadata is usually not encrypted. It does not provide access to the content of a message, but it can provide information on identity, location, and colleagues. Data analytics techniques can process metadata to identify an individual against whom more assertive techniques (such as operations to gain access to their device) can then be used in order to access content, but these assertive techniques can be both expensive and risky.

In general, intelligence agencies have a greater ability to gain access to plaintext than law enforcement agencies. The fewer legal constraints there are on an agency, individual, or country, the more likely they are to find some way to defeat encryption and gain access to plaintext. The United States and other Western democracies limit what actions their agencies can take against citizens by imposing restrictions on intelligence activities that are essential to protect civil liberties. U.S. intelligence agencies, for example, are not bound by the same legal constraints as law enforcement agencies when it comes to pursuing foreign targets, but their domestic activities are restricted in ways that prevent them from collecting data on criminal activity unrelated to foreign intelligence or sharing information with law enforcement agencies.

Interviews with NSA officials suggest that the agency is reluctant to undertake a domestic mission that could divert resources away from its foreign intelligence responsibilities. NSA does not want to be placed in a position where it may have to reveal its techniques in court, nor meet stringent judicial standards for chain of custody. Nor, given its authorities, can the NSA "service" cases that do not involve foreign intelligence in some way. One issue for consideration is whether the United States should expand the remit of intelligence agencies to support law enforcement or whether it should allow law enforcement agencies to develop similar hacking capabilities.[2]

There are other techniques that are time intensive or data intensive that require specialized skills and equipment. What is difficult for the NSA may be impossible for the FBI, given both legal and

2. See Cryptome, "Catch Him with His Encryption Down: Counter-Encryption Techniques in Child Exploitation Investigations," https://cryptome.org/isp-spy/crypto-spy.pdf, for a discussion of forensic and investigatory techniques.

operational constraints. In the United States, most of these techniques would require considerably more resources for law enforcement agencies and would raise ethical and legal issues. To use the cryptanalytic techniques discussed above, law enforcement agencies would need to be more like signals intelligence agencies and, even with the requirement for court approvals for such operations, there could be serious risks to civil liberties.

06

# Options for Managing the Encryption Problem

The central dilemma in dealing with encryption is that it is in the interest of privacy and national security to encourage widespread use of encryption, but some kinds of encryption unavoidably complicate the tasks of law enforcement investigations and intelligence collection. Any response needs to take into account the fact that the same technologies that empower criminals and terrorists to evade detection or launch malicious attacks can also provide enormous benefits with respect to security, privacy, and the economy. Finding a sustainable solution will require policymakers to consider the interests of companies, law enforcement, and consumers. We are in a world of second-best solutions, and movement on encryption will require compromises that balance competing political forces, both domestic and international.

There are three broad categories of options for managing the encryption problem: a laissez faire approach, the imposition of restrictions on unrecoverable encryption, or finding alternative ways for law enforcement agencies to access digital evidence (essentially increasing their ability to hack endpoints). The following sections discuss these options, but should not be construed as an endorsement of any of these approaches.

A laissez faire approach would allow companies to sell whatever kind of encryption they think the market will buy. This is the default option, and it is what we have now. A problem with this approach is that it may not be sustainable internationally. The life of the laissez faire option can be prolonged by the usual Washington theatrics of commissions, enquiries, special committees, and other mechanisms to give the appearance of movement, but it is ultimately untenable. There will be continued pressure from law enforcement agencies in the United States and elsewhere to prevent further erosion of their investigative and prosecutorial capabilities.

Restricting the design, production, sale, or use of unrecoverable encryption faces insurmountable political obstacles in the United States. This includes bans on the use of unrecoverable encryption, mandating that companies build products that permit lawful access or data recovery, or requiring both telecom and Internet service providers to enable access or block certain encryption products. Some of these measures, besides being politically unpalatable in the United States, could

prompt a reaction in the global IT market against U.S. products that could produce real economic harm to the nation.

It is also important to recognize that this will not solve all of the problems for law enforcement and intelligence agencies. While roughly half of the 546 foreign encryption products identified in a recent survey are from countries that mandate recoverability,[1] the other half are not, and no matter what international agreement is reached, malicious actors will find ways to access unrecoverable encryption through apps produced outside of the agreement or open source and self-made encryption applications. Restricting encryption could also push companies toward other technical solutions to evade the reach of law enforcement, including storing data overseas and not collecting or storing customer data.

The option that poses fewer political difficulties is to expand law enforcement capabilities to exploit vulnerabilities to compromise devices and applications pursuant to investigations, in other words, lawful hacking. There are a number of ways to do this. One way is to allow agencies to purchase hacking services or tools and then use them under existing oversight and approval procedures. There are concerns that getting law enforcement agencies into the business of hacking could be unethical, but the FBI already employs endpoint breaches (called network investigative techniques) under a degree of court oversight. The attraction of improving law enforcement capabilities to hack or decrypt target devices or traffic is that it would not place limitations on how companies design their systems or on what types of products or services consumers are able to use.

Law enforcement agencies already have some legal authorities and technologies to hack endpoint devices, and while adopting endpoint hacking by law enforcement agencies as a primary means of evidence collection could raise concerns, there is room to do more with existing authorities. In the short term, the FBI should invest in more technical resources and find new ways to employ skilled hackers consistent with oversight requirements. However, lawful hacking is not a perfect solution. Relying on this approach could create an arms race dynamic between law enforcement and companies that could quickly escalate costs for both sides. Jurisdictional issues also arise if the sought-after data is located outside of the United States.

Other capabilities can also help law enforcement agencies, such as tools to analyze metadata. Greater use of metadata can provide additional investigative avenues to law enforcement. Metadata can include location data, call records, and e-mail header information, but it does not include the substance of a call or message. As more devices are connected to the Internet, the amount of data generated by individuals will grow, offering greater opportunities to establish patterns of behavior. While metadata is useful, it cannot fully replace the content of communications as evidence. For example, it can show that two people communicated around the time of an incident, but it cannot show what they said, which is critical to proving intent.

1. Bruce Schneier, "Worldwide Encryption Products Survey," *Schneier on Security* (blog), February 11, 2016, https://www.schneier.com/blog/archives/2016/02/worldwide_encry.html.

Congress could clarify the scope of law enforcement's existing authorities under the Communications Assistance for Law Enforcement Act (CALEA).[2] CALEA was written in the pre-Internet age, and as a result its mandates do not cover over-the-top service providers and mobile operating system providers. CALEA also does not require service providers to decrypt (or provide the ability to decrypt) communications unless the carrier provided the encryption method and has the ability to decrypt traffic. CALEA could be modernized and expanded, but amendments to CALEA would be difficult to push through Congress.

Another way to expand law enforcement capabilities would be to remove legal obstacles to expanded NSA support for law enforcement. Intelligence agencies often use techniques unavailable to law enforcement agencies, and one issue for consideration is whether we should expand the remit of intelligence agencies to support law enforcement or whether we should allow law enforcement agencies to develop similar hacking capabilities.[3] In the United States, NSA would need different authorities and perhaps additional resources, and the use of classified programs would face problems with discovery by defense lawyers and chain of custody issues for evidence. Furthermore, many of NSA's most effective techniques for gaining access to data cannot be used on U.S. citizens, which could limit its ability to support law enforcement.

A final option would be to create new national organizations for decryption support to law enforcement. Such a center could leverage existing federally funded research and development centers (FFRDCs) or research universities. Several of these already have programming expertise and advanced computing equipment, which could be leveraged by state and local law enforcement to access additional decryption capabilities and resources.

Any new organization would require the development of mechanisms to ensure coordination at the federal, state, and local levels. An FFRDC or university would need additional resources to create decryption centers. It might be possible to enlist the assistance of some IT companies in this domestic and regional effort. Distributing encryption support among universities in different regions or states might also make this option attractive to Congress.

The principle drawback of this approach, however, is that it is unlikely to ameliorate the problem. It is unrealistic to expect research universities and FFRDCs to maintain an edge against the global tech industry that would allow them to consistently break commercial encryption. These centers would have to constantly find new ways to break encryption, as their sources and methods would be regularly revealed by exposure in court and companies would continue to develop new encryption methods. Making FFRDCs responsible for decryption services would divert resources such as supercomputers and elite computer scientists away from other valuable projects that support day-to-day needs of law enforcement.

A complicating factor in all this is that we should not count on the rest of the world to wait for the United States to find its way to a solution. China and Russia are unlikely to wait, nor will American

2. See appendix B for additional information on CALEA.

3. See Cryptome, "Catch Him with His Encryption Down: Counter-Encryption Techniques in Child Exploitation Investigations," https://cryptome.org/isp-spy/crypto-spy.pdf, for a discussion of forensic and investigatory techniques.

policy create precedents for their actions. In contrast, Western countries still look to the United States, but they have begun to implement national solutions independent of U.S. action, chiefly data localization and decryption assistance requirements. Encryption in this regard is an element of the larger collision between national law and global networks. The worst outcome would be a pastiche of regulations or measures that would unfairly target U.S. companies.

07

# Balancing Individual Rights and the Social Good

We can draw several conclusions from our research into encryption use. First, it is in the national interest to encourage the use of strong encryption. No one interviewed in the law enforcement or intelligence communities disagreed with this. Saying that agencies want to weaken encryption is either a misunderstanding or a misrepresentation.

Second, the encryption challenge to public safety comes primarily from two kinds of products and services, those for instant messaging and for full disk encryption that do not allow for recovery of unencrypted data without the consent of the user. These are fast growing offerings, and decisions by a few companies will have a profound effect on what kind of encryption consumers use.

Third, the risk to public safety created by the use of such products has not reached a level that justifies restrictions or design mandates. Data on the number of cases and investigations thwarted by encryption is partial and incomplete, but indicates that a only small percentage of cases are affected.

Fourth, the use of unrecoverable encryption is a global issue complicated by foreign concerns over the dominance of American IT companies, the continued high risk of terrorism, concerns over corruption, and weak oversight of law enforcement monitoring in many important emerging markets, and the battle between authoritarian regimes and democracies over how human rights apply to the Internet. Perversely, unrestricted access to unrecoverable encryption creates greater risk for democracies than for authoritarian regimes, which are largely unconstrained in their ability to surveil communications, whether or not encryption is used.

Fifth, demand for unrecoverable encryption is driven by a perceived risk to privacy and by the hope that offering unrecoverable products and services will benefit American companies in a global market. Both the risk to privacy and the risk to US companies' foreign markets from concern about government surveillance are overstated. Our review of the change in revenue for leading IT companies as a result of the Snowden leaks suggests that concerns about U.S. government surveillance did not create insurmountable headwinds to U.S. companies.[1] Interviews with foreign

1. See Appendix A for a discussion of the effects of the Snowden leaks on U.S. tech companies.

officials suggest that the American privacy community is more vocal than is the case in other democracies (with the possible exception of Germany), and much more influential in shaping policy and law. This disparity in influence will hamper that ability of the United States to develop globally acceptable encryption policies, and whatever decision the United States makes now on encryption policy will not be the final decision.

Finally, the debate over encryption is the most salient part of a broader debate on social responsibility on the Internet. The laissez-faire approach of letting companies and consumers do whatever they want is under global challenge. Encryption policy is part of a larger debate on how to define the responsibilities of citizens, companies, and governments in cyberspace. The old free-wheeling Internet where governments were superfluous is ending,[2] but societies have not defined what will take its place. Governments are developing the tools and techniques to assert sovereignty and are reasserting responsibility for central functions like security and law enforcement. They are extending sovereign control using privacy laws, data localization, and requirements for cybersecurity. A central part of this debate is who controls online data and what rules should apply to it.

If everyone in the world used unrecoverable encryption, what would change? Greater encryption use could help reduce cybercrime, which costs the world economy at least $400 billion per year,[3] and also reduce the risk of cyber attack. Privacy protection would improve. These benefits must be weighed against the cost to public safety. In any case, everyone will not use unrecoverable encryption. Companies and consumers continue to demand features enabled by recoverable encryption. Our research suggests that the scope and use of unrecoverable encryption, while frustrating to law enforcement, is small and its risk is manageable.

Law enforcement agencies are justifiably concerned that this could change rapidly, driven by consumer preferences for mobile messaging services and the ease of acquiring unrecoverable encryption. Our research suggests that the market will continue to prefer using recoverable encryption for e-mail and enterprise networks. Two other technologies define the parameters of the encryption problem: full disk encryption for mobile devices and end-to-end encryption for instant messaging. Our analysis of market share and trends suggests that the share of mobile devices and apps that employ unrecoverable encryption is likely to continue to grow.

Encryption lets individuals and companies better control their own data, but the extent and nature of this control is not fully defined. Companies may prefer encryption products that avoid placing them in difficult jurisdictional battles over data or where they are seen, to their detriment in the market, as agents of government. Some consumers will prefer encryption that blocks law enforcement access, but citizens do not have the right to total privacy.[4] Some countries use data and encryption policies as a barrier to trade. Developing a sustainable encryption policy requires

2. John Perry Barlow, "A Declaration of the Independence of Cyberspace," Electronic Frontier Foundation, February 8, 1996, https://www.eff.org/cyberspace-independence.

3. James Lewis and Stewart Baker, *The Economic Impact of Cybercrime and Cyber Espionage* (Santa Clara, CA: McAfee/CSIS, 2013), http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf.

4. United Nations, "Universal Declaration of Human Rights," December 10, 1948, http://www.un.org/en/universal-declaration-human-rights/. The declaration bars "arbitrary interference with an individual's privacy," and the Fourth Amendment prohibits "unreasonable searches."

considering more than the ability of law enforcement to investigate and prosecute crime, although this currently is the most salient issue.

The question is what encryption policy best allows people to live safely and freely. Drawing on the precedent of the Fourth Amendment to the U.S. Constitution and the United Nations' Universal Declaration of Human Rights, the answer is neither the complete absence of restriction nor a guarantee of total access for government. We need to balance the rights of the individual with the needs of public safety in the use of new and valuable technology. There is still time to develop national and international policies that create this balance, but that time is not unlimited. This issue will come to a head as more devices connect to the Internet (the so-called Internet of Things), greatly magnifying the scope of the problem.

# Appendix A. Effect of Snowden Leaks on U.S. Tech Companies

The revelation of Edward Snowden about U.S. intelligence activities in May 2013 caused U.S. IT companies understandable concern, as foreign governments and consumers became suspicious of U.S. products. A desire to deflect this suspicion explains in part the emphasis on making "government proof" encryption available.

The extent to which the Snowden revelations have affected U.S. tech companies is subject to debate. One estimate published in 2013, immediately after the Snowden revelations, suggested that the U.S. cloud services industry could lose $35 billion dollars by 2016.[1] However, the U.S. cloud industry experienced consistent growth over the last three years. Top cloud providers like Amazon Web Services (AWS) and Microsoft Azure have grown at a rapid pace. AWS revenue grew nearly 70 percent in 2015,[2] while Microsoft reported Azure revenues increased by 140 percent.[3] That said, it is possible that they would have grown even faster if not for the Snowden leaks.

The broader tech sector has struggled in recent years, with a strong dollar, weak global growth, and declining smartphone demand all putting pressure on revenue growth. Looking at the revenue of the top 10 U.S. tech companies,[4] growth has weakened significantly over the last five years, but the bulk of the decline pre-dated the Snowden revelations, and growth actually recovered over the next few quarters following the leaks before resuming its decline.

Anecdotal data suggests that the reaction to Snowden has presented challenges to some companies. Microsoft and Amazon have reported losing clients to foreign competitors, and foreign

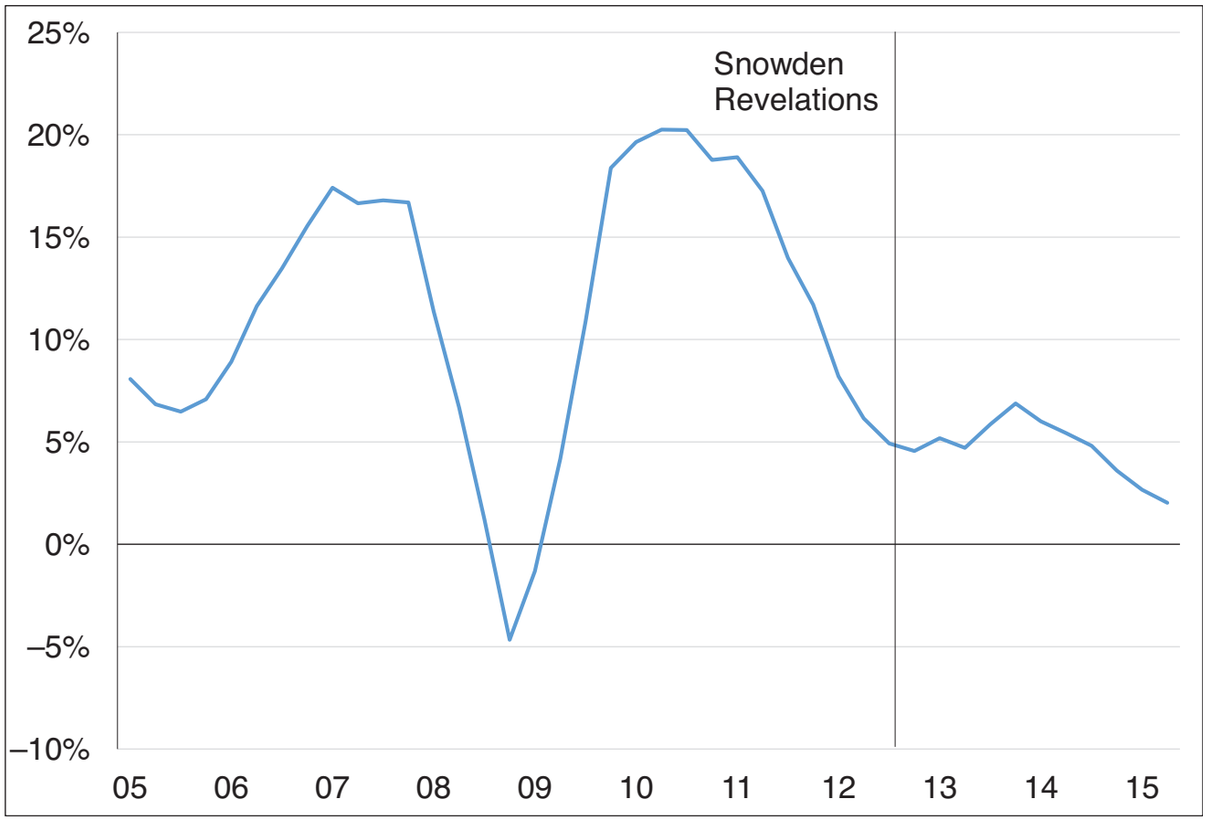
1. Daniel Castro, "How Much Will PRISM Cost the U.S. Cloud Computing Industry?," Information Technology & Innovation Foundation, August 2013, http://www2.itif.org/2013-cloud-computing-costs.pdf.

2. Statista, "Quarterly Revenue of Amazon Web Services from 1st Quarter 2014 to 2nd Quarter 2016 (in million U.S. dollars)," http://www.statista.com/statistics/250520/forecast-of-amazon-web-services-revenue/.

3. Microsoft, "Earnings Release FY16 Q2," January 28, 2016, https://www.microsoft.com/en-us/Investor/earnings/FY-2016-Q2/press-release-webcast.

4. See Fortune 500's list of U.S. tech companies by revenue, available at http://beta.fortune.com/fortune500/list/filtered?sector=Telecommunications.

## Figure A.1. Year-Over-Year Revenue Growth of Top 10 U.S. Tech Companies




Source: According to Fortune 500's list, the top 10 U.S. tech companies by revenue are currently Apple, Amazon, HP, Microsoft, IBM, Alphabet, Intel, Cisco, Oracle, and Qualcomm. http://beta.fortune.com/fortune500/list/filtered?sector=Telecommunications. Revenue data aggregated by CSIS from YCharts company data, Revenue Quarterly, https://ycharts.com/companies/revenues.

customers ranging from German software companies to the government of India have decided to cancel contracts with American cloud providers.[5] IBM has invested more than $1 billion in overseas data centers for clients who fear sending their data to the United States.[6] Other companies, meanwhile, have adopted new encryption features to demonstrate their commitment to protecting their customers' data.[7] But some companies offer a more sanguine view; for example, Cisco reported that deals have been slower to close since the revelations, but have still ultimately gone through.[8]

5. Claire Cain Miller, "Revelations of N.S.A. Spying Cost U.S. Tech Companies," *New York Times*, March 21, 2014, http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html; Gerry Smith, "'Snowden Effect' Threatens U.S. Tech Industry's Global Ambitions," *Huffington Post*, January 24, 2014, http://www.huffingtonpost.com/2014/01/24/edward-snowden-tech-industry_n_4596162.html.

6. Miller, "Revelations of N.S.A. Spying Cost U.S. Tech Companies."

7. Claire Cain Miller, "Angry over U.S. Surveillance, Tech Giants Bolster Defenses," *New York Times*, October 31, 2013, http://www.nytimes.com/2013/11/01/technology/angry-over-us-surveillance-tech-giants-bolster-defenses.html.

8. Miller, "Revelations of N.S.A. Spying Cost U.S. Tech Companies."

While there is some evidence that concerns about U.S. government surveillance are complicating international sales efforts for U.S. tech companies, there is no clear evidence of a shock to the sector's revenue.

The Snowden revelations contributed to policy decisions by a few large governments to emphasize data localization, increase reliance on domestic services rather than U.S. providers (e.g., Schengen net), increase privacy protections and redress, and in some instances to create domestic industries to build alternatives to American products. Perhaps the greatest challenge comes from the Chinese government, with its plans to displace foreign IT providers and create Chinese companies that are global competitors, using subsidies and nontariff barriers to trade. While there is debate about the ability of the Chinese to make competing products, the near-term effect is to move sales away from U.S. companies and to threaten future global market share.

Offering end-to-end encryption appears to not affect these decisions, suggesting that it is unlikely to protect companies from foreign governments adopting policies that hurt their market share. However, an announcement by the United States that it will require American-made encryption products and services to provide for lawful access would likely only reinforce anti-American sentiment.

The growing concern in many key nations about the security risks associated with unrecoverable encryption could lead them to ban products and services that are inaccessible to law enforcement, resulting in complete loss of market access for American service providers that offer unrecoverable encryption. This reinforces the need for common understanding among nations on encryption as a prerequisite for effective policy.

# Appendix B. Surveillance Statutes: CALEA and the All Writs Act

Federal statutes that provide the legal authority and capability to collect electronic evidence have not kept pace with technology. This applies to wiretaps of real-time communications as well as access to stored communications on personal devices and in the cloud.

In 1994, Congress enacted the Communications Assistance for Law Enforcement Act (CALEA), which required telecommunications providers to assist law enforcement in executing court authorized electronic surveillance of real-time communications. The statute requires covered telecommunications providers to build in wiretapping capabilities for law enforcement's lawful intercept and evidence collection needs.[1] CALEA applies to traditional telecommunications carriers and providers, voice over Internet protocol (VoIP) services, and broadband access services, but the law has three important exceptions.

First, the law explicitly provides that it does not authorize law enforcement to require any specific design of equipment, systems, or facilities, nor does it prohibit the adoption of particular technologies by providers. Second, it does not apply to many communications services that were created after the law was passed and have since become popular platforms to communicate and distribute content. These include what are called over-the-top (OTT) communications services and applications that Internet service providers are neither responsible for nor able to control. In mobile communications, such apps include WhatsApp, Snapchat, Facebook Messenger, iMessage, Facetime, Telegram, and many others. Third, CALEA explicitly provides that telecommunications carriers are not responsible for decrypting communications for law enforcement when they do not possess the key. This means that CALEA authorities do not apply to OTT communications apps that offer encryption.

Stored data, particularly data stored in the cloud, is currently more accessible to law enforcement. Most cloud providers maintain the ability to decrypt data as most of their customers still expect to be able to recover data if they forget their password or other credentials. But rapid adoption of full

1. 47 U.S. Code § 1002, https://www.law.cornell.edu/uscode/text/47/1002.

disk encryption on mobile phones and other consumer devices is a significant challenge to law enforcement access to electronic evidence.

Unable to access locked mobile devices seized as part of a crime scene using their own capabilities, law enforcement has sought assistance from device manufacturers using authority derived from the All Writs Act of 1789, which provides federal courts the authority to compel third parties to assist in the execution of a court order. A prime example is the application of the All Writs Act in a case involving Apple and the FBI's investigation of Syed Rizwan Farook in the aftermath of the 2015 San Bernardino attack.[2] The FBI sought to compel Apple to assist in providing access to the data on Farook's iPhone, which was fully encrypted and included authentication features that prevented the FBI from obtaining the encryption key. Application of the All Writs Act largely hinged on whether the request would impose an unreasonable burden on Apple and whether compelling this type of assistance would be consistent with the intent of Congress. The legal battle over this became moot when the FBI hired a third party to hack the phone.

2. Robert Chesney and Steve Vladeck, "A Coherent Middle Ground in the Apple-FBI All Writs Act Dispute?," *Lawfare*, March 21, 2016, https://www.lawfareblog.com/coherent-middle-ground-apple-fbi-all-writs-act-dispute.

# About the Authors

**James A. Lewis** is a senior vice president at CSIS, where he writes on technology, security, and innovation. Before joining CSIS, he worked at the Departments of State and Commerce as a Foreign Service officer and as a member of the Senior Executive Service. His government experience includes work on a range of politico-military and Asian security issues, as a negotiator on conventional arms transfers and advanced military technology, and in developing policies for satellites, encryption, and the Internet. Lewis led the U.S. delegation to the Wassenaar Arrangement Experts Group on advanced civil and military technologies and was the rapporteur for the 2010, 2013, and 2015 UN Group of Government Experts on Information Security. He was also assigned to U.S. Southern Command for Operation Just Cause and to U.S. Central Command for Operation Desert Shield. He received his Ph.D. from the University of Chicago.

Lewis is an internationally recognized expert on cybersecurity. Lewis is the U.S. lead for a long-running Track II Dialogue on cybersecurity with the China Institutes of Contemporary International Relations. He has authored numerous publications on the relationship between technology, innovation, and national power. Other reports written by Lewis examine the role of space in national security. His current research examines international security and governance in cyberspace, the relationship between innovation and technology, the future of warfare, and the effect of the Internet on politics. He has served as a member of the Commerce Department's Spectrum Management Advisory Committee and the State Department's Advisory Committee on International Communications and Information Policy, and as a member and chair of the Advisory Committee on Commercial Remote Sensing. Lewis is frequently quoted in the press and has testified numerous times before Congress.

**Denise E. Zheng** is a senior fellow and director of the Technology Policy Program at CSIS, where her work is focused on cyber and emerging technology issues. Previously, she served as chief of staff and lead science and engineering technical adviser as a contractor for the Defense Advanced Research Projects Agency (DARPA) foundational cyber warfare program, Plan X. Before DARPA, Ms. Zheng was director for global government relations and cybersecurity policy at CA Technologies

where she advised company executives on cybersecurity, data security and breach notification, and software assurance. While at CA, she was a member of the Information Technology (IT) Sector Coordinating Council, IT Information Sharing and Analysis Center, and SAFECode.

Prior to CA Technologies, Ms. Zheng served as a professional staff member for the Senate Homeland Security and Governmental Affairs Committee. In that role, she was a principal in drafting and negotiations for comprehensive cybersecurity legislation and conducted oversight of critical infrastructure protection programs, spectrum auctions, privacy, and federal IT programs. Ms. Zheng previously held various positions at CSIS, including program manager of the Technology and Public Policy Program, where she managed the CSIS Cybersecurity Commission among other program initiatives. In addition to writing on technology and cybersecurity issues, she has also authored reports on U.S.-China relations and soft power, and civil space policy issues. Ms. Zheng holds a B.A. in economics and political science from the University of Michigan, studied government at the London School of Economics and Political Science, and completed graduate coursework in security studies at the Johns Hopkins University School of Advanced International Studies.

**William A. Carter** is an associate fellow in the Technology Policy Program at CSIS. His work focuses on international cyber policy issues, including data localization, surveillance and privacy, cyber conflict and deterrence, financial sector cybersecurity, and encryption. Before joining CSIS, he worked as a financial analyst in the Goldman Sachs Investment Strategy Group, advising private and institutional clients on their short- to medium-term asset allocation decisions. In this role, he performed research and analysis on all investable asset classes, as well as geopolitics and the macro economy, and produced reports and presentations on international affairs and current events. He has interned at the Council on Foreign Relations and at Caxton Associates, a New York hedge fund. He graduated from New York University in 2010 with a B.A. in economics.