BSA BACKGROUND PAPER:

Encryption and Law Enforcement Access to Data

As policy discussions around the use of encryption and law enforcement's ability to access digital evidence return to the spotlight, this white paper providers an overview of key issues. Since the Federal Bureau of Investigation (FBI) initiated a lawsuit seeking to force decryption of a smart phone recovered from the suspect in the 2015 terrorist shooting in San Bernardino, California, substantial new information has come to light that speaks to the scale of access challenges, the potential efficacy of mandatory decryption (or "exceptional access"), and the vital role of encryption in securing cyberspace. These developments point the way to win-win solutions that can improve law enforcement access to digital evidence while sustaining strong cybersecurity.

Summary

- Proposals for mandatory exceptional access to encryption fundamentally pit the costs of potentially weakening security against the perceived benefits of improving law enforcement access to encrypted data.
- Recent developments in the security environment demonstrate that **the costs of weakening encryption have risen**; meanwhile, recent data indicates that law enforcement challenges in accessing encrypted data may be less significant than previously asserted.
- **Encryption is fundamental to effective cybersecurity**; it is a critical element in securing the most sensitive data, networks, and devices — including critical infrastructure networks, identity information, 5G networks, and IoT devices.
- It is widely agreed that **proposals to mandate third-party access to encryption would inevitably weaken cybersecurity**; such proposals raise a host of questions about the need for, viability of, and benefits of taking such action.
- **There are promising alternatives to improve law enforcement access to data while maintaining cybersecurity and privacy;** law enforcement and technology communities should work together to explore these options.

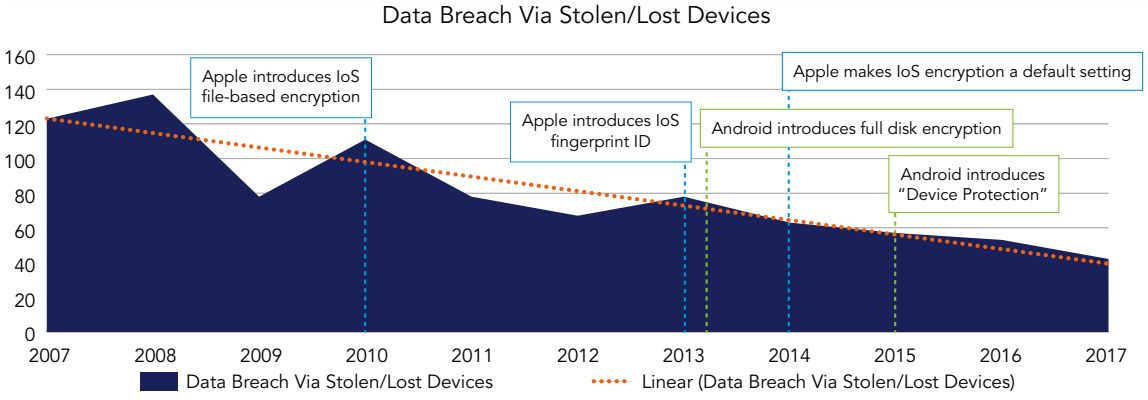
Encryption Is a Vital Tool in Today's Evolving Security Environment

- **Encryption secures critical infrastructure, which is under attack with growing frequency and impact.** Recent large-scale cyber attacks have cost the global economy several billion dollars and demonstrated the growing potential of cyber weapons to disrupt critical services. A 2018 survey reports that 90 percent of global critical infrastructure operators have been damaged by cyber attacks within the previous two years. In March 2018, the Department of Homeland Security warned that a nation-state actor had "targeted government entities and multiple U.S. critical infrastructure sectors, including the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors" for sophisticated cyber attacks. Encryption plays a key role in securing critical infrastructure by protecting sensitive data, authenticating authorized users, and securing network traffic.

- **Encryption is a critical defense against massive data breaches.** The breach of over 143 million unencrypted financial records held by the credit scoring company Equifax in 2017 highlights the growing problem of massive data breaches exposing individuals' sensitive data, often facilitating identity theft and other crimes. According to the latest *Breach Level Index*, 2,600,968,280 records were breached in 2017. Of these, 96.9 percent of the breached records were unencrypted, demonstrating how essential encryption is to limiting the harm caused by breaches. Moreover, encryption of mobile devices has led to a precipitous decline in breaches occurring when malicious actors accessed lost or stolen devices (see **Figure 1**). In addition to preventing breaches of stolen devices, and affiliated networks or systems encryption actually deters theft: data indicates that, in the 6 months after Apple introduced its "Activation Lock" mechanism, iPhone thefts declined by 38 percent in San Francisco, 19 percent in New York, and 24 percent in London. Smartphone theft has dropped 50 percent in the United Kingdom since 2012 (Activation Lock was introduced in 2013).

- **End-to-end encryption will play a vital role in securing 5G and the Internet of Things (IoT).** 5G networks will transmit massive amounts of data, create complex and decentralized interconnections among devices, operate with exponentially higher speeds and lower latency, and introduce new network architectures and use cases. 5G technology will form

Figure 1. Device encryption has substantially diminished data breaches.



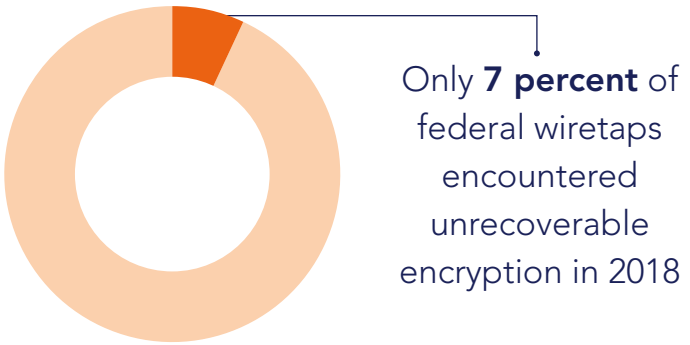
Source: Adapted from "The Evolution of Data Leaks," *Wired*, November 2017.

the backbone of the IoT. Meanwhile, IoT devices are rapidly proliferating — experts have estimated that as many as 20 billion IoT devices will be online by next year. These devices handle massive volumes of data, often sensitive data such as personal information or critical infrastructure data, and present alarming vulnerabilities unless that data is secured. Common to both 5G and the IoT is the need for decentralized, multi-layered approaches to security in addition to traditional network-based defenses. Encryption will be an essential element of this new security architecture. It will secure data wherever it travels, support strong authentication of authorized users in diverse computing environments, and authenticate software updates to keep the vast network of largely autonomous IoT devices secure. In fact, encryption is so important to IoT security that NIST's draft Core Cybersecurity Feature Baseline for Securable IoT Devices (NIST Interagency Report 8259) includes cryptographic data protection as one of six core security features recommended for all IoT devices, and has been identified as a vital priority in IoT security guidance issued by the Internet Engineering Task Force, the IoT Security Foundation, the Open Web Application Security Project, and the Trusted Computing Group, among others.

Law Enforcement Faces Challenges in Accessing Certain Data, But Is Not "Going Dark"

- **Law Enforcement access challenges are real, but encryption is not the primary problem.** Though encryption can be used to secure devices, web traffic, and communications such as emails, it is not universally prevalent. A 2017 CSIS report estimated that, globally, only 21 percent of mobile devices use unrecoverable encryption and only 18 percent of internet communications traffic uses unrecoverable encryption. Reports on law enforcement wiretaps by the Administrative Office of the U.S. Courts also provide insight into the prevalence of the challenge: in 2018, less than 7 percent of the nearly 3,000 state and federal wiretaps encountered unrecoverable encryption (see **Figure 2**). Not surprisingly, in a 2015 study of law enforcement challenges in accessing digital evidence sponsored by the Bureau of Justice Assistance, a survey of law enforcement personnel identified 34 distinct challenges — including insufficient law enforcement understanding of how to handle digital evidence and how to frame requests to providers — but encryption was not ranked among the top tier.

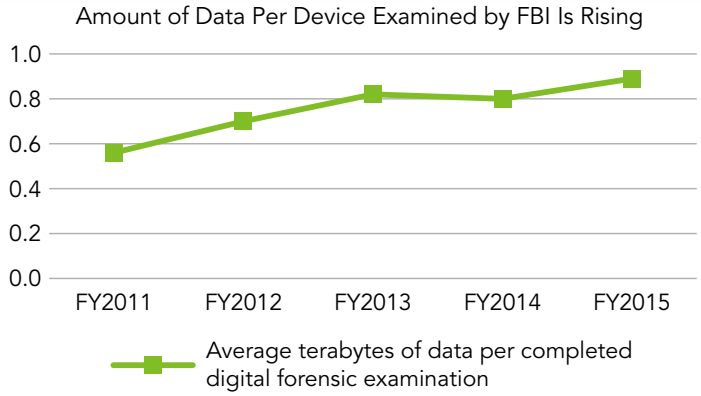
Figure 2. Unrecoverable encryption impacts a small percent of state and federal wiretaps.



Source: U.S. Courts, *Wiretaps Report 2018*.

- **Widely cited statistics on inaccessible devices were inaccurate.** In a series of public speeches in 2017 and 2018, Justice Department and FBI officials claimed that federal law enforcement had been unable to access nearly 8,000 encrypted devices connected to criminal investigations. After a *Washington Post* expose, the FBI acknowledged the true number was only a fraction of those claimed — likely around 1,200 devices. Likewise, after the FBI claimed it was unable to access a phone connected to the 2015 San Bernardino shooting, the FBI Inspector General found that the FBI had failed to explore available technical options for accessing the phone even while key FBI officials knew of a vendor that had almost completed work on a solution.

Figure 3. Use of data in criminal investigations is rising.



Source: FBI Regional Computer Forensics Laboratory FY 2013 and 2015 Annual Reports.

- **The volume and types of new data online make the 21st century a "golden age" for law enforcement access.** Even as encryption usage has grown, vast new data sets have become available to law enforcement, providing law enforcement with powerful new tools. Geolocation data, personal data (such as health tracking, financial transactions, and transportation routes), internet search data, and social media postings, among other sources, provide law enforcement with treasure troves of potential evidence. IBM estimates that 2.5 *quintillion* bytes of new data are generated each day. The tremendous volume of law enforcement requests to technology providers offers some sense of this boon. For example, in 2018, law enforcement and government agencies issued over 153,000 requests for data from four major technology providers — Microsoft, Apple, Google, and Facebook — seeking data for 367,648 unique identifiers. Over that time period, the providers satisfied 85 percent of these requests.

- **Governments have demonstrated success in accessing encrypted communications without mandated back-doors.** Governments have demonstrated that they have tools and techniques to access encrypted communications without the need for exceptional access mandates. U.S. law enforcement organizations have invested millions of dollars to obtain tools from providers like Cellebrite and GrayKey that allow the agencies to access encrypted devices. Court filings demonstrate that the FBI has also achieved recent successes in accessing encrypted messages on the text messaging service Signal. And the Dutch government demonstrated its ability to access encrypted messages through an operation to intercept an encryption server, making over 250,000 messages accessible. As these examples demonstrate, law enforcement has taken advantage of an array of methodologies to access encrypted data both at rest and in transit, all without mandating exceptional access.

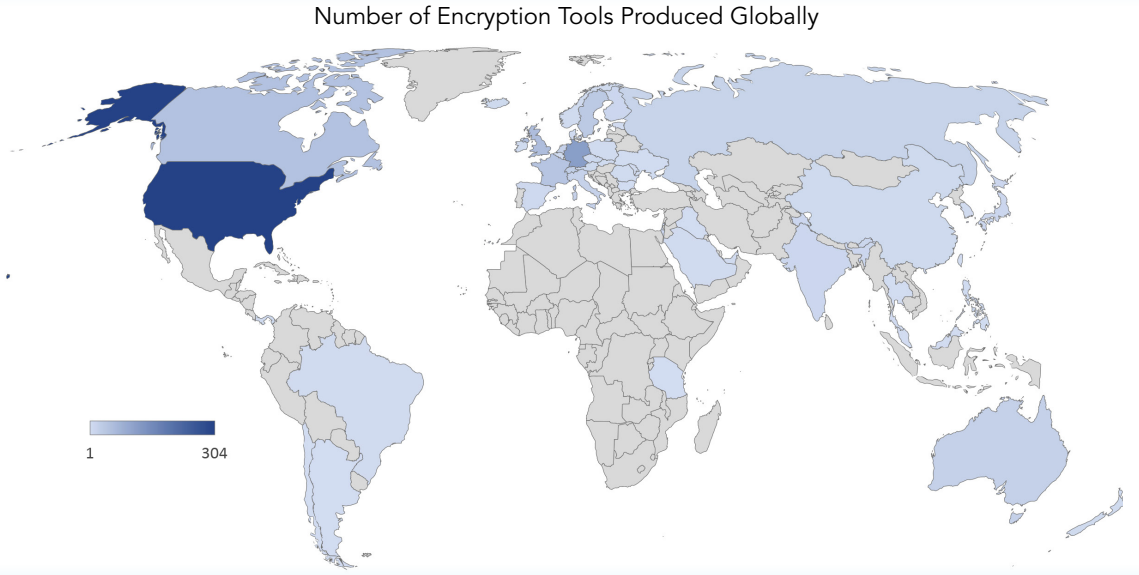
Mandated Government Access Is Not a Viable Solution

- **Experts have repeatedly warned that mandated access to encryption would inevitably weaken cybersecurity.** An expert task force convened by the National Academies of science concluded in 2018 that, "Exceptional access features, no matter how well designed and implemented, will reduce their security to some degree as a result of the added complexity and greater potential for weaknesses in their design, implementation, or operation." This task force joined several other examinations of the issue in that conclusion. A 2015 report by a number of leading computer scientists, "Keys Under Doormats," found that exceptional access approaches "pose far more grave security risks, imperil innovation on which the world's economies depend, and raise more thorny policy issues than we could have imagined when the Internet was in its infancy." And a report by the Center for Internet Security noted that mandated exceptional access "would not guarantee" consistent law enforcement access to encrypted communications, "and yet it would harm the data security of countless average, law-abiding people."

- **Weakening encryption and data security would have a broad impact.** It would weaken national security by enabling adversaries to exploit encryption to access military secrets and sensitive communications. It could enable industrial espionage against American businesses, generating billions of dollars in damage to the national economy. And it could enable oppressive regimes to target human rights defenders and democracy advocates, undermining freedom globally.

- **Domestic encryption legislation would push malicious actors to use widely available foreign or homegrown technologies that aren't subject to U.S.** law. Encryption technology is a global industry, often open source, and malicious actors are using homegrown and foreign-sourced encryption. A *2016 survey of worldwide encryption products* found 865 hardware or software products incorporating encryption, of which two-thirds were produced outside of the United States (See **Figure 4**). These products were produced in 55 different countries including countries from every continent other than Antarctica. As a report by the Heritage Foundation noted, "Even if Congress mandates some sort of special access, there is no guarantee that it would be the effective solution law enforcement wants, since criminals and terrorists could just buy different products that do not have a backdoor." Moreover, 44 percent of these products are available to the public for free, and over a third are open source, meaning that individuals can adapt the products by modifying or adding to the code. Indeed, the terrorist group ISIS has been found to use a free open-source product generated from unknown actors known as TrueCrypt, the freely available Russian-developed service Telegram, and an apparently self-produced encrypted messaging app called Alrawi.apk, among others. Al Qaeda has also reportedly developed and deployed its own encryption tool, originally called Mujahedeen Secrets, based on open source encryption products.

Figure 4. At least 55 countries produce encryption tools.



Source: *A Worldwide Survey of Encryption Products*, 2016.

- **Encryption technology is evolving rapidly and will outpace legislated solutions.** Changes in technologies, threats, and customer needs drive rapid evolution in encryption technologies, and coming innovations will make mandated exceptional access solutions less viable and more likely to weaken security. Homomorphic encryption, which allows for processing of encrypted data without requiring decryption, quantum encryption, which uses light photons to transmit sensitive data, and quantum-proof encryption, which uses encryption algorithms to secure data against the powerful decryption capabilities of quantum computers, will all offer substantial security benefits against growing threats, but will also make exceptional access more technically challenging. This technological evolution means that mandating exceptional access will not only weaken current security tools, but also risk undermining innovations that could prevent future threats.

Law Enforcement Can Improve Ability to Access Data Without Undermining Encryption

- **Expanding and improving technical training should be an urgent priority.** As the Center for Strategic and International Studies noted in a recent report, "Knowledge of digital systems and how to access, handle, and utilize digital evidence is increasingly important to virtually every type of criminal case, but dedicated training in evidence handling, recovery, analysis, and storage is limited." Though training is available through a number of public and private providers, it is not accessed by sufficient numbers of law enforcement personnel to bridge the gap. One challenge is simply the multiplicity — and, potentially, redundancy — of providers: the federal government alone provides technical training to federal, state, and local law enforcement personnel through at least five separate organizations, most of them small in size and serving niche audiences. Consolidating, expanding, and codifying

these technical training platforms to bring a more strategic and visible approach to technical training could pay major dividends. Moreover, additional resources to support these kinds of trainings are needed at the federal, state, and local levels.

- **Insufficient digital crime-fighting Infrastructure creates major investigative challenges.** A lack of capacity in digital forensics labs, insufficient or outdated forensic equipment, and too few trained forensic examiners can create major delays in accessing and analyzing digital evidence. One digital forensics firm's 2016 survey of nearly 500 law enforcement agencies found that most agencies reported a backlog, and 38 percent reported backlogs ranging from 3 months to over a year. When digital forensics laboratories face such lengthy backlogs, hundreds or thousands of devices will sit on storage room shelves while investigations stall. To address this challenge, greater investment in digital crime-fighting infrastructure, including additional forensic labs, cutting edge digital forensics equipment, and trained lab technicians and forensic examiners, is sorely needed.

- **Industry is working to support law enforcement investigations.** As law enforcement officers navigate the ever-evolving multitude of digital platforms, configurations, and applications to seek digital evidence, they constantly turn to the technology community for assistance. Yet, collaboration is challenged by a lack of understanding on both sides of the procedures and constraints of their counterparts. For example, law enforcement officials often lack understanding of how to accurately describe data sets they seek, or how to target requests narrowly enough to enable a speedy response. Industry leaders are already working to bridge this gap, and some technology providers lack sufficient infrastructure to effectively address requests. For example, Apple announced in 2018 that it was creating "a team of professionals dedicated solely to training law enforcement officials around the world" as well as "an on-line training module for law enforcement." Certainly, there is more to be done to establish standardized procedures for collaborating on lawful investigations and to identify common challenges and best practices. BSA has recently published its "BSA Global Best Practices for Law Enforcement Access to Digital Evidence," which includes best practices for both law enforcement and technology providers, in support of this priority.