CLCT

WILLIAM & MARY LAW SCHOOL

Cybersecurity and Information Security Newsletter

Issue 2 | August 3, 2020

Please feel free to submit cybersecurity and information security news items or request related topics to Daniel Shin (dshin01@wm.edu).

Lawful Access to Encrypted Data Act

Lawful Access to Encrypted Data Act

On June 23, 2020, a bill "Lawful Access to Encrypted Data Act," S. 4051, 116th Cong. (2020), available here, (the "Bill") was introduced in the Senate. The Bill attempts to reconcile the public's interest in strong encryption with law enforcement's desire to lawfully obtain encrypted data. It is intended to provide law enforcement with the ability to view encrypted data. The Bill would force some technology companies to assist law enforcement in decrypting private data when presented with a court-issued search warrant. To do that, the companies would need to have the necessary technological capabilities in place to permit rapid reaction to a future search warrant.

- The Bill allows a court to "order a device manufacturer, an operating system provider, a provider of remote computing service, or another person" to prepare "all information, facilities, and assistance necessary to access information stored on an electronic device or to access remotely stored electronic information." This may include decrypting information, "*unless the independent actions of an unaffiliated entity make it technically impossible to do so.*" (emphasis added)
- It requires device manufacturers selling over one million devices per year, operating system providers, and providers of remote computing services to have the capability to assist law enforcement in the presence of a valid search warrant.
- Finally, the Bill authorizes the Attorney General to issue directives, under certain circumstances, to compel private parties to report "any technical capabilities that the person knows or expects to be necessary to implement and comply with an anticipated court order or other lawful authorization" and "the timeline of the person for developing and deploying the technical capabilities."

Legal Background

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The "basic purpose of this Amendment," the Supreme Court has recognized, "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) (quoting Camara v. Mun. Court City & Cty. San Francisco, 387 U.S. 523, 528 (1967)), available here.

"It is a cardinal rule that, in seizing goods and articles, law enforcement agents must secure and use search warrants wherever reasonably practicable. . . . This rule rests upon the desirability of having magistrates rather than police officers determine when searches and seizures are permissible and what limitations should be placed upon such activities. . . . To provide the necessary security against unreasonable intrusions upon the private lives of individuals, the framers of the Fourth Amendment required adherence to judicial processes wherever possible. And subsequent history has confirmed the wisdom of that requirement." Chimel v. California, 395 U.S. 752, 758-59 (1969), available here.

The Fourth Amendment protects against unreasonable searches and seizures by government officials. It empowers law enforcement officials with wide powers to search and seize

individuals and their property, if there is a valid warrant granted by an independent magistrate judge who determined that there is a probable cause of evidence of a crime.

Background on Encryption

Currently, commercial operators and private individuals in the U.S. can freely use strong encryption technologies and are not required to integrate encryption backdoors (e.g., key escrow or key recovery systems) in anticipation of a lawful search warrant issued by a court.

Encryption has been traditionally regulated under export controls to prevent other nations, such as the former Soviet Union, from obtaining U.S. technologies that could enhance their military potential. Although using encryption has not been illegal within the U.S., transferring encryption technology abroad or disclosing the technology to non-U.S. persons required an export license under certain circumstances. *See* Exec. Order No 13,026, 61 Fed. Reg. 58,767 (Nov. 15, 1996), available here. However, the use of encryption within the nation has been left to data users.

The U.S. government does not dispute the necessity of using encryption for commercial activities, but it has consistently expressed its concerns about the use of encryption for unlawful activities. For example, the National Security Agency has previously fought against efforts to make strong encryption technology available for the public because it argued that it would hamper the government's efforts "to stop terrorists and child pornographers." *See* Daniel R. Rua, Comment, *Cryptobabble: How Encryption Export Disputes Are Shaping Free Speech for the New Millennium*, 24 N.C. J. Int'l L. & Com. Reg. 125, 132 (1998), available here.

Bill: Analysis and Implication

The Bill attempts to accomplish two main goals. First, to clarify the role of device manufacturers and information service providers (the "Providers") on how to assist law enforcement in the presence of a court order compelling disclosure of information, including encrypted information. Anticipating situations where information is encrypted beyond the Providers' control, the Bill explicitly does not make the Providers liable for their inability to decrypt data that they hold.

Second, the Bill obliges major Providers *to be ready* to assist law enforcement even prior to a search warrant being issued. During search warrant operations, time is often of the essence, so the Bill requires Providers to be readily available when a court issues a search warrant.

The Bill does not impose an obligation on Providers to create new backdoors to facilitate warrant-based search and seizure operations. However, it may force Providers to do so as a pragmatic matter in order to comply with the proposed statutory duty to assist in decrypting data. It may also force Providers to disclose existing technologies embedded in their devices and services that could serve as a backdoor to decrypt information. For example, cell phone manufacturers may be forced to disclose firmware update mechanisms to law enforcement, because a carefully crafted firmware update can provide a surreptitious means to monitor a target device.

If enacted, the Bill would encourage Providers to shift away from privacy-centric systems and move towards surveillance-permissive information systems.

- *The Bill is likely to conflict with certain cybersecurity best practices.* The "trust-no-one" principle to encryption holds that only the encrypted data owner, not the Providers, has possession of the decryption keys. If Providers are bound to assist law enforcement in accessing encrypted data, they will not be able to offer services using this principle. Device products and services will likely have weaker cybersecurity safeguards to comply with the Bill's provisions.
- *There is a risk that the Bill may open avenues for other countries to demand access to encrypted data.* If Providers implement technologies that could decrypt encrypted data for U.S. law enforcement, then law enforcement from other countries may also compel Providers to decrypt data under the countries' respective legal standards for search and seizure. If proper jurisdictional requirements are met, multinational Providers may face legal compulsion to disclose decrypted data to other countries, including those with lower legal standards for lawful search and seizure than in the U.S. It is arguable that the Bill may open the floodgates to a host of decryption orders by other governments, which may encourage Providers to streamline the decryption process while discouraging the implementation of strong encryption security for their customer's data.

The Bill contemplates scenarios in which a third party implements additional layers of encryption outside of the Provider's control. Specifically, Providers are not to be held liable if data encrypted by "the independent actions of an unaffiliated entity make it technically impossible" to be accessed. Lawful Access to Encrypted Data Act, S. 4051, 116th Cong. (2020).

The Bill may also have the unintended side effect of bolstering small device manufacturers whose annual sales are below one million devices because they would not be required by the Bill to have the capability to assist law enforcement for decrypting data. Thus, small-scale device manufacturers, such as startups funded via Kickstarter (a crowdfunding platform) could legally manufacture highly secure electronic devices with no backdoors, without violating the terms of the Bill.

Except when a Provider receives a directive from the Attorney General, the cost of complying with the Bill, if enacted, would be the responsibility of the Providers as a cost of doing business.

Read the press release by the U.S. Senate Committee on the Judiciary here.