Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

February 22, 2021

Law Enforcement and Technology: the "Lawful Access" Debate

Technological advances present both opportunities and challenges for U.S. law enforcement. For example, some developments have increased the quantity and availability of digital content and information for investigators and analysts. Some observers say law enforcement's investigative capabilities may be outpaced by the speed of technological change, preventing investigators from accessing certain information they may otherwise be authorized to obtain. Specifically, law enforcement officials cite strong, end-to-end encryption, or what they have called *warrant-proof* encryption, as preventing lawful access to certain data. Companies employing such strong encryption have stressed they do not hold encryption keys. This means they may not be readily able to unlock, or decrypt, the devices or communications—not even for law enforcement presenting an authorized search warrant or wiretap order.

Front Door or Back Door Access

Rhetoric around the encryption debate has focused on the notion of preventing or allowing *back door* access to communications or data. Many view a back door as the ability for an entity, including a government agency, to access encrypted data without the user's explicit authorization. However, back door access can be a security vulnerability. Despite this concern, a number of encrypted products and services have built-in back doors and thus can comply with law enforcement requests for information. For instance, many email service providers encrypt email communications and also maintain a key to those communications stored on their servers. This is also the case for cloud providers that maintain keys to the data stored on their servers. Strong, end-to-end encryption where companies do not maintain keys, however, does not contain the same opportunities for access. Also, unintended back doors, or vulnerabilities, may be discovered by technology companies, security researchers, government investigators, malicious actors, or others.

Law enforcement contends that they want *front door* access, where there is a clear understanding of when they are accessing a device, as the notion of a back door sounds secretive. This front door could be opened by whomever holds the key once investigators have demonstrated a lawful basis for access, such as probable cause that a crime is being committed. Whether front or back, however, building in an encrypted door that can be unlocked with a key—no matter who maintains the key—adds a potential vulnerability to exploitation by hackers, criminals, and other malicious actors. Researchers have yet to demonstrate how it would be possible to create a door that could only be accessed in lawful circumstances.

CALEA

The simultaneous opportunities and challenges that evolving technology present to law enforcement have received congressional attention for several decades and have been a central point of contention between law enforcement and technology companies.

The 1990s brought concerns that digital and wireless communications made it more difficult for law enforcement agencies to execute authorized surveillance. In response, Congress passed the Communications Assistance for Law Enforcement Act (CALEA; P.L. 103-414) to help law enforcement maintain its ability to execute authorized electronic surveillance. Among other things, CALEA requires that telecommunications carriers assist law enforcement in efforts to intercept electronic communications for which it has a valid court order to carry out. There are several noteworthy exceptions to this requirement:

- Law enforcement cannot require (or prohibit) providers of wire or electronic communications services (as well as manufacturers of equipment and providers of support services) to implement "specific design of equipment, facilities, services, features, or system configurations." In other words, they cannot require providers to build in access points.
- Telecommunications carriers are not responsible for decrypting any encrypted communications (or ensuring that the government has the ability to do so), unless the company already has the ability to do so.
- CALEA applies to telecommunications carriers but specifically does not apply to "information services" such as websites and internet service providers. (Notably, the Federal Communications Commission administratively expanded CALEA's requirements to also apply to certain broadband and Voice over Internet Protocol [VoIP] providers.)

Proposed expansions of CALEA generally fall into two broad categories. Some proposed expansions may broaden the range of communications or information service providers covered by CALEA. Some have been interested in making CALEA more technology neutral, such that it could, given the rapidly changing technology landscape, apply to a wider range of communications or information service providers. Other expansions may broaden the requirements placed on telecommunication carriers—such as maintaining the ability to decrypt communications—placed on entities covered by CALEA.

Crypto Wars

Around the time that policymakers were passing CALEA, a larger discussion on encryption was taking place. The so-called crypto wars pitted the government against data privacy advocates in a debate on the use of data encryption. This tension was highlighted by law enforcement proposals to build back doors to certain encrypted communications devices as well as to block the export of strong encryption code.

Clipper Chip. During the Clinton Administration, encryption technology, known as the Clipper Chip, was introduced. This technology used a concept referred to as *key escrow*. The idea was that the Clipper Chip would be inserted into a communications device, and at the start of each encrypted communication session, the chip would copy the encryption key and send it to the government to be held in escrow, essentially establishing a back door for access. With authorization—such as a court authorized wiretap—government agencies would then have the ability to access the key to the encrypted communication. Vulnerabilities in the system design were later discovered, showing that the system could be breached and the escrow capabilities disabled; as such, this system was not adopted.

Encryption Export. Pretty Good Privacy (PGP) encryption software was a widely used email encryption platform and was considered a milestone because it made military-grade cryptography available to the public. PGP proliferated when someone released a copy of it on the internet, sparking a federal investigation into whether PGP's creator was illegally exporting cryptographic software (then considered a form of "munitions" under U.S. export regulations) without a specific munitions export license. Ultimately, the case was resolved without an indictment.

Renewed Crypto Wars?

The debate over law enforcement's lawful access to encrypted information originally focused on data in motion, or real-time communications. More recent technology changes have potentially affected law enforcement capabilities to access not only real-time communications but stored content, or data at rest. A central element of the debate now involves determining what types of information law enforcement is able to access and under what circumstances.

Communications content. Wiretap requests are submitted by law enforcement to judges, requesting permission to intercept certain wire, oral, or electronic communications in transit. In 2019, federal and state judges authorized 3,225 wiretaps, of which there were 464 instances reported to the Administrative Office of the U.S. Courts in which encrypted communications were encountered. Law enforcement could not decrypt the content in 438 (approximately 94%) of the cases where they encountered encrypted communications.

Call Detail Records. Law enforcement may request, with a subpoena or valid court order, certain call detail records from telecommunications providers. These records can include information such as the sending and receiving telephone numbers, whether or not the call was completed, call duration, and which cell towers were used to make or receive the call. These may be available retrospectively or sometimes in real time. Companies vary in the length of time they maintain call detail records and other data such as GPS location information. Notably, call detail records do not contain the *content* of telephone calls.

Stored Data. With a warrant or subpoena, law enforcement may attempt to obtain data stored in the cloud or on a device.

- Ease of law enforcement access to cloud-based data may depend on factors including the location of the cloud server, the service provider, and length of time information has been stored in the cloud. If the server is located overseas, for instance, law enforcement can employ the Mutual Legal Assistance process to try to obtain the data from a partner nation. Factors that may limit the scope of data stored in the cloud (and subsequently, availability to law enforcement) include whether individuals store data in or back up their devices to the cloud and whether cloud storage space and backup schedules capture the full range of data.

- With respect to devices, access to devices and the content on them may be locked and encrypted. Various factors can affect law enforcement's efforts to gain access to a device and its contents. For instance, law enforcement attempting to unlock a device with *brute force* would likely use software to try every possible combination of keys in an attempt to unlock the device. The success of this method may depend, among other things, on the amount of time available to try and unlock a device, device limits on passcode attempts, and the number of keys used in the passcode.

Going Forward

Policymakers may evaluate the extent to which end-to-end encryption affects law enforcement investigations and public safety. They may weigh this against privacy and data security concerns as they consider whether to expand or curtail law enforcement's lawful access to certain information. Changes could involve incentives or requirements for communications and technology companies to provide specified information to law enforcement, enhanced investigative tools, bolstered financial and manpower resources to help law enforcement better leverage existing authorities, or combinations of these and other options.

For additional resources, see CRS Report R44481, *Encryption and the "Going Dark" Debate*; CRS Report R44187, *Encryption and Evolving Technology: Implications for U.S. Law Enforcement Investigations*; and CRS Report R44827, *Law Enforcement Using and Disclosing Technology Vulnerabilities*.

Kristin Finklea, Specialist in Domestic Security

IF11769

Disclaimer