CRS INSIGHT

Renewed Crypto Wars?

February 9, 2016 (IN10440)

Related Author

- Kristin Finklea

Kristin Finklea, Specialist in Domestic Security (kfinklea@crs.loc.gov, 7-6259)

Technology has been evolving at a rapid pace, presenting both opportunities and challenges for U.S. law enforcement. On the one hand, some contend that technology developments have resulted in a "golden age of surveillance" for law enforcement; the large amount of information that investigators have at their fingertips—access to location data, information about individuals' contacts, and a range of websites—collectively form "digital dossiers" on individuals. On the other hand, some argue that law enforcement is "going dark" as their capabilities are outpaced by the speed of technological change, and thus they cannot access certain information they are authorized to obtain. Strong encryption, for instance, has been cited as one such innovation contributing to law enforcement's going dark issue.

While the tension created by changing technology is not new, it was reinvigorated in 2014 as technology companies like Apple and Google began implementing automatic enhanced encryption on mobile devices and certain communications systems. Companies using such strong encryption do not maintain "back door" keys and therefore cannot unlock, or decrypt, the devices—not even when presented with an authorized wiretap order. Concerns about the lack of back door keys were highlighted by the November and December 2015 terrorist attacks in Paris, France and San Bernardino, CA. Questions arose as to whether the attackers used strong encryption and, more importantly, if they did, whether this prevented law enforcement and intelligence officials from identifying the attackers and potentially thwarting the attacks. These questions have reopened discussions on how encryption and quickly advancing technologies could impact law enforcement investigations.

Crypto Wars

In the 1990s, a broad discussion on encryption took place in the United States. The "crypto wars" pitted the government against data privacy advocates in a debate on the use of data encryption. This strain was highlighted by proposals to build back doors into certain encrypted communications devices and 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 called "key escrow." The idea was that a chip (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. During the same period, the federal government opened an investigation into Philip Zimmermann,

the creator of Pretty Good Privacy (PGP) encryption software, the most widely used email encryption platform. When PGP was released, it "was a milestone in the development of public cryptography. For the first time, military-grade cryptography was available to the public, a level of security so high that even the ultra-secret code-breaking computers at the National Security Agency could not decipher the encrypted messages." When someone released a copy of PGP on the Internet, it proliferated, sparking a federal investigation into whether Zimmermann was illegally exporting cryptographic software (then considered a form of "munitions" under the U.S. export regulations) without a specific munitions export license. Ultimately the case was resolved without an indictment. Courts have since been presented with the question of how far the First Amendment right to free speech protects written software code—which includes encryption code.

CALEA

The 1990s also brought "concerns that emerging technologies such as digital and wireless communications were making it increasingly difficult for law enforcement agencies to execute authorized surveillance." 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 in a changing technology environment. Among other things, CALEA requires that telecommunications carriers assist law enforcement in executing authorized electronic surveillance.

There are several noteworthy caveats to the requirements under CALEA:

- Law enforcement and officials may *not* require telecommunications providers (and manufacturers of equipment and providers of support services) to implement "specific design of equipment, facilities, services, features, or system configurations." Similarly, officials may *not* prohibit "the adoption of any equipment, facility, service, or feature" by these entities.
- Telecommunications carriers are not responsible for "decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication."

Congressional Action

Both CALEA caveats play central roles in the current debate. For one, policymakers have been questioning whether to require certain entities to build back doors in their products and services such that law enforcement could more easily access communications and data when presenting a lawful wiretap order or warrant. Further, they have been debating the utility of requiring these entities to ensure that devices and communications could be unlocked and decrypted. Questions regarding potential legislation include

- would legislation be effective if it can only impose requirements on products manufactured or sold in the United States;
- would back doors allowing exceptional access for one entity—law enforcement—inadvertently allow exceptional access for others;
- could legislation be sufficiently technology neutral to keep pace with technological change;
- what economic impact might back door requirements have on affected U.S. technology companies; and
- would allowing the U.S. government access to certain communications and devices set the desired example for other governments?

The Obama Administration considered pushing for legislation requiring technology companies to build back door access points into encryption but decided against it. In the absence of a favorable legislative option, some have proposed a national commission to study today's security and technology challenges and to brainstorm options that might be acceptable to both law enforcement and the technology industry.