CRS INSIGHT

Paris Attacks and "Going Dark": Intelligence-Related Issues to Consider

November 19, 2015 (IN10400)

Related Policy Issue

- Intelligence and National Security

Related Author

- Anne Daugherty Miles

Anne Daugherty Miles, Analyst in Intelligence and National Security Policy (amiles@crs.loc.gov, 7-7739)

Authorities are tracking numerous individuals involved in the deadly assault in Paris on November 13, 2015. According to one report, "a rogues' gallery of homegrown terrorists with links to Islamist groups has become large enough — and is acting stealthily enough — to make tracking them increasingly difficult for the region's intelligence agencies." (See CRS Insight IN10209, *European Security, Islamist Terrorism, and Returning Fighters*, by Kristin Archick and Paul Belkin.)

While CRS has found no specific evidence of encrypted communications linked to the Paris attacks cited in news reports, some are using the Paris attacks to highlight the difficulties of collecting intelligence when communications data can be encrypted—an issue called "going dark." On November 16, 2015, Central Intelligence Agency (CIA) Director John Brennan stated:

[O]peratives and terrorist networks ... have gone to school on what it is that they need to do in order to keep their activities concealed from the authorities.... [T]here are a lot of technological capabilities that are available right now that make it exceptionally difficult, both technically as well as legally, for intelligence and security services to have the insight they need to uncover it.

"Going Dark"

Technology changes have impacted law enforcement capabilities to access (1) communications in transit between devices and (2) stored data within devices. Companies such as Apple and Google have announced that they cannot unlock their devices for anyone under any circumstances, not even for law enforcement (because they do not maintain a key to decrypt messages sent between their devices.)

Lawfare's Benjamin Wittes explains the encryption problem this way:

It's about data at rest on devices, data that is now being encrypted in a fashion that can't easily be cracked when those

devices are lawfully seized. And it's also about data in transit between devices, data encrypted such that when captured with a lawful court-ordered wiretap, the signal intercepted is undecipherable....

Initial recruitment may take place on Twitter, but the promising ISIS candidate quickly gets moved onto messaging platforms that are encrypted end to end. As a practical matter, that means there are people in the United States whom authorities reasonably believe to be in contact with ISIS for whom surveillance is lawful and appropriate but for whom useful signals interception is not technically feasible.

Issues for Congress

A number of hearings have focused on the subject of "going dark." On July 8, 2015, the Senate Judiciary Committee and Senate Select Committee on Intelligence held separate hearings with James Comey, Director of the Federal Bureau of Investigation (FBI). Comey framed the core question: "Once all of the requirements and safeguards of the laws and the Constitution have been met, are we comfortable with technical design decisions that result in barriers to obtaining evidence of a crime?"

Organizations such as the American Civil Liberties Union (ACLU) are vocal in their opposition to any action that might weaken encryption technologies. According to the ACLU: "Such proposals threaten privacy and place an improper burden on private entities to build the government's surveillance infrastructure, decrease cyber and national security, and are unnecessary given current law enforcement access to electronic information."

In commentary on the Paris attacks, Michael Morrell, former Deputy Director of the CIA and currently Senior Counselor for Beacon Global Strategies LLC, said, "We have ... had a public debate [about encryption].... defined by Edward Snowden ... and the concern about privacy. I think we're now going to have another debate ... defined by what happened in Paris." (In 2013, Edward Snowden's release of thousands of classified National Security Agency [NSA] documents prompted demands for greater privacy protections primarily within the context of intelligence counterterrorism and law enforcement activities.)

The terrorist attacks in the United States on September 11, 2001 (9/11), prompted a new look at legislation related to surveillance and search provisions. Congress passed the Foreign Intelligence Surveillance Act (FISA) in 1978 to provide a statutory framework regulating when government agencies may gather foreign intelligence through electronic surveillance or physical searches. A number of laws passed after 9/11 amended FISA to enable the government to obtain information in a greater number of circumstances. (Major revisions are associated with P.L. 107-56, P.L. 108-458, and P.L. 110-261.) Most recently, the USA FREEDOM Act (P.L. 114-23) was signed into law on June 2, 2015. The principal focus of the legislation was to address the bulk collection of telephone metadata by the NSA. (See CRS Legal Sidebar WSLG1278, *USA FREEDOM Act Reinstates Expired USA PATRIOT Act Provisions but Limits Bulk Collection*, by Edward C. Liu.)

Some have dubbed the Paris attacks the "French 9/11." Intelligence and law enforcement communities across the globe have expressed concerns about the "going dark" problem. The attacks may create a difficult challenge for Congress: experts note that surveillance laws will have to balance current concerns about emerging technologies with the need to keep Americans safe and protect American privacy and civil liberties.

Recent events may spark renewed debate concerning surveillance provisions in FISA (or other laws authorizing electronic surveillance, such as the Communications Access for Law Enforcement Act [CALEA, P.L. 103-414]). For more on "going dark" and CALEA, see CRS Report R44187, *Encryption and Evolving Technology: Implications for U.S. Law Enforcement Investigations*, by Kristin Finklea.

The Paris attacks illustrate that the United States is not alone in its efforts to balance privacy and security. FBI Director Comey's testimony points out the global nature of this challenge:

It is clear that governments across the world, including those of our closest allies, recognize the serious public safety risks if criminals can plan and undertake illegal acts without fear of detection.... We should be clear that any steps that we take here in the United States may impact the decisions that other nations take.... In addition, any next steps we identify will be more effective if we are working together with our allies, and made more difficult if we are isolated.