Fact Sheet: Section 215 of the USA PATRIOT Act

CSIS csis.org/analysis/fact-sheet-section-215-usa-patriot-act

February 27, 2014

Issue: Section 215 of the USA PATRIOT Act has been used to collect, in bulk, telephony metadata of U.S. persons and U.S. Citizens.

Background: Section 215, also known as the "Tangible Things" or "Business Records" provision of the USA PATRIOT Act, amended Section 501 of the Foreign Intelligence Surveillance Act and permits the collection of "…tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information…" The collection of such items is permitted if the investigation seeks to obtain foreign intelligence information that does not concern U.S. persons. If it the information sought does relate to a U.S. person, it must be relevant to preventing terrorism or espionage, and not be based solely upon activities protected by the first amendment. To prevent improper utilization of the data, Section 215 requires the adoption of specific minimization procedures, which have been outlined in recently declassified Foreign Intelligence Surveillance Court (FISC) orders. This provision of the PATRIOT Act has been interpreted to permit the bulk collection of "telephony metadata," or the mass collection of basic call-log information, from telecommunications companies. This includes the date, time, and duration of calls to and from all phone numbers. This telephony metadata does not include specific personally identifying information such as the names or addresses connected to the phone numbers. If a problem is found with a particular number, and the number is believed to be attributed to a U.S. person, that informationis passed to the FBI, which must then use publicly available information, either through other sources of intelligence or court orders, to connect the number with subscriber information.

Controversy: The bulk collection of metadata under Section 215 is one of the most controversial aspects of the NSA's intelligence collection activities. Critics argue metadata can reveal the most intimate details of an individual's life, and that because the 215 collection program indiscriminately sweeps up the data of U.S. citizens, it violates Fourth Amendment protections against warrantless search and seizure. The long list of "tangible things" the government can seek excites critics, who fear government overreach. Critics also argue Section 215 has not been an effective counterterrorism tool.

Assessment: There are legitimate operational reasons for the bulk collection of data. Unlike law enforcement investigations, which analyze crimes retrospectively (that is after they have been committed), counterterrorism intelligence collection focuses on preventing attacks in the future. Information must be collected prospectively to be effective. Good intelligence is

built upon the accumulation of information from multiple sources, both big and small, and often of ambiguous significance. There are rarely any 'smoking-guns.' Removing any single intelligence capability from the threat detection picture could limit the IC's ability to protect the nation in the future. Intelligence analysis is like looking at a jigsaw puzzle and guessing the picture when you don't have all the pieces. That makes every piece you do have useful.

Section 215 has been reviewedandrenewed by Congress twice since 2006. The Supreme Court has held that phone records are not considered private or privileged information for Fourth Amendment purposes because they are voluntarily provided to telecommunications carriers for billing purposes. As of July 31, 2013, the FISC had reauthorized the program 34 times under 14 different judges. More recently, however, two federal judges came down on opposite sides of the issue. Judge Richard K. Leon of the District of Columbia District Court ruled the 215 collection program illegal, while Judge William H. Pauley of the Southern District of New York upheld the legality of the programs.

Despite the breadth of data collected, it has rarely been accessed. In 2012, the NSA queried 288 primary phone numbers, and through contact chain analysis touched 6,000 numbers. Overall, Section 215 data has contributed intelligence to 12 counterterrorism cases with a potential homeland nexus.

Section 215 bulk data is protected against misuse through multiple oversight mechanisms, including minimization procedures that seek to restrict the retention of certain classes of data, like U.S. person data, and internal personnel controls to limit access to the data. To ensure continued program relevance and compliance with established parameters, the 215 collection program is reviewed for reauthorization every 90 days by the FISC, and reports are filed with the court every 30 days. Review by the House and Senate Permanent Select Committees on Intelligence provide an additional layer of oversight. In total, since 2003, there have been 12 confirmed cases of intentional misuse of collected signals data (not necessarily related to 215), most of which were targeted at a personal connection or romantic interest of an individual analyst. Since 2009 there have been a few isolated unintentional incidents of data misuse, only two of which represented broader Section 215 rules violations.

In the first instance, 3000 call detail records over five years old, which had not been properly disposed of in accordance with minimization procedures, were discovered on an NSA server. The records were not accessible for intelligence analysis, and were deleted upon discovery. In the second incident, the NSA received customer credit card information from a telecommunications company after the company made an unannounced software change, which altered the data delivered to the NSA. Upon discovering the unrequested data, the NSA concealed the data from intelligence analysis access, and later deleted it. All of other reported incidents were small, incidental, and resulted in the imposition of measures to prevent repetition in the future. Even very minor incidents were recorded and duly reported to the FISC.

Scott F. Mann is a research associate with the Strategic Technologies Program at the Center for Strategic and International Studies (CSIS) in Washington, D.C.

Commentary

Scott F. Mann

Media Queries

Contact H. Andrew Schwartz
Chief Communications Officer
Tel: 202.775.3242

Contact Paige Montfort
Media Relations Coordinator, External Relations
Tel: 202.775.3173