GlobalResearch
Center for Research on Globalization

Police State Surveillance under the US Patriot Act: Congress Should End Telephone Metadata Collection

By Prof. Marjorie Cohn
Global Research, May 13, 2015
Truthout 12 May 2015

Region: USA
Theme: Intelligence, Law and Justice, Police State & Civil Rights

Image: Senate Majority Leader Mitch McConnell (R-Kentucky) disputed a federal appeals court ruling on Thursday that the National Security Agency's bulk collection of phone records is illegal, and some senators expect McConnell to try for a short-term extension of the existing law. (Photo: Doug Mills/The New York Times)

Just as Congress was debating whether to reauthorize Section 215 of the Patriot Act, which the government has used to collect data on every telephone call we make, the Second Circuit Court of Appeals unanimously struck it down in ACLU v. Clapper. Congress has four days left in its current session to decide whether to reauthorize Section 215, amend it or let it die a natural death on June 1, 2015 (the date on which it will sunset if not reauthorized).

Section 215 of the Patriot Act

The controversial section authorizes the Foreign Intelligence Surveillance Court (FISC) to issue orders mandating phone companies, internet service providers, banks, credit card companies etc. to provide their records to the government if the FISC finds "there are reasonable grounds to believe" the records "sought are relevant to an authorized investigation" aimed at protecting the country "against international terrorism."

Thanks to Edward Snowden, we know that the FISC used Section 215 to issue an order mandating Verizon to provide

> "on an ongoing daily basis … all call detail records or 'telephony metadata' … for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls."

The National Security Agency (NSA) has been collecting metadata on our phone communications, including the identities of the caller and the person called, the phone numbers of both parties, as well as the date, time, duration and unique identifiers of the communication.

The "data archive" could be accessed only "when the NSA has identified a known telephone number for which … there are facts giving rise to reasonable, articulable suspicion that the telephone number is associated with [Redacted]." The Court of Appeals speculated that the Redacted portion "presumably" includes "terrorist activity or a specific terrorist organization."

So the government is collecting data that is not "relevant to an authorized investigation," but it argues that it might be of use later when a specific terrorist suspect or terrorist plot is being investigated.

The government "does not seriously dispute [the] contention that all significant service providers in the United States are subject to similar orders," Judge Gerard E. Lynch wrote for the three-judge panel of the Court of Appeals in *Clapper*. That means all of our phone communications are being collected.

The Court of Appeals Opinion

Judge Lynch began by citing *United States v. U.S. Dist. Court (Keith)*, in which the Supreme Court in 1972 struck down warrantless surveillance procedures that the government had argued were lawful as an exercise of the president's power to protect national security. The *Keith* Court remarked on "the inherent vagueness of the domestic security concept [and] the necessarily broad and continuing nature of intelligence gathering."

Lynch went on to describe the Senate's Church Committee, established in response to *Keith* and alleged abuses in the intelligence-gathering and surveillance activities of the NSA, FBI and CIA during "the early 1970s, in a climate not altogether unlike today's." The committee concluded that the privacy rights of US citizens had been violated by activities conducted under the rubric of foreign intelligence collection.

It was the *Keith* case together with the findings of the Church Committee that led Congress in 1978 to enact the Foreign Intelligence Surveillance Act (FISA) and establish the FISC to review the government's applications for wiretap orders. The FISC, which functions in secret, has authorized just about every wiretap the government has asked for since its creation.

Shortly after the September 11, 2001, attacks, Congress amended FISA by passing the USA Patriot Act, and subsequently amended Section 215. An application for a wiretap order must contain

> "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) … to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." (emphasis added).

In construing the phrase, "relevant to an authorized investigation," Lynch notes, "The records demanded are all-encompassing; the government does not even suggest that all of the records sought, or even necessarily any of them, are relevant to any specific defined inquiry."

The government argued that although the vast amount of information does not contain directly "relevant" information, the data should be collected as it may allow the NSA sometime in the future to identify relevant information. Lynch disagreed, noting, "We agree with appellants that such an expansive concept of 'relevance' is unprecedented and unwarranted."

Lynch observed,

> "The sheer volume of information sought is staggering; while search warrants and subpoenas for business records may encompass large volumes of paper documents or electronic data, the most expansive of such evidentiary demands are dwarfed by the volume of records obtained pursuant to the orders in question here."

But, Lynch noted,

> "§ 215 does not permit an investigative demand for any information relevant to fighting the war on terror, or anything relevant to whatever the government might want to know. It permits demands for documents 'relevant to an authorized investigation.'"
>
> "The overwhelming bulk of the metadata … concerns … individuals who are not targets of an investigation or suspected of engaging in any crime whatsoever, and who are not even suspected of having any contacts with any such targets or suspects,"

Lynch wrote.

The court was concerned about the slippery slope of allowing the government such expansive power to collect our data. "If the government is correct," Lynch noted,

> it could use § 215 to collect and store in bulk any other existing metadata available anywhere in the private sector, including metadata associated with financial records, medical records, and electronic communications (including e-mail and social media information) relating to all Americans."

"Such expansive development of government repositories of former private records," according to Lynch, "would be an unprecedented contraction of the privacy expectations of all Americans."

The court held that Section 215 does not authorize the government "to collect phone records only because they may become relevant to a possible authorized investigation in the future."

Therefore, the court decided that Section 215 "does not authorize the telephone metadata program." Since the Court of Appeals concluded that Section 215 does not allow the FISC order, it did not decide whether the metadata collection program also violates the US Constitution.

Because Section 215 is set to expire soon, and Congress is debating how to proceed, the Court of Appeals decided not to issue a preliminary injunction at this time. The court's opinion rejected the government's contention that Congress impliedly authorized the FISC order when it voted for extensions of Section 215. The court said that since the metadata program was secret, members of Congress could not be said to have approved it.

Judge Robert D. Sack concurred with Lynch's opinion and wrote separately, "Because our decision is based on our reading of a federal statute, not the Constitution, Congress can in effect overrule it." If the Court of Appeals had instead concluded that the metadata collection program violated not just Section 215, but the Fourth and/or First Amendments to

the US Constitution as well, Congress would be bound by that decision.

What Should Congress Do?

The House of Representatives is poised to pass the USA Freedom Act of 2015, which would amend Section 215 to end bulk collection of metadata from domestic phone companies, but would leave in place a sweeping surveillance program focused on international communications. And if a call originates overseas, information about Americans could still be collected. It would allow the NSA to continue to analyze the metadata, which would be stored by the telephone companies. A panel of experts would advise the FISC, but there would be no provision for a civil liberties advocate. The House Judiciary Committee rejected amendments that would provide safeguards for civil liberties and require the government to secure a warrant before searching collected data for information about Americans.

Even before the Court of Appeals issued its ruling, senators were at odds about what to do with Section 215. Many of them, including Sen. Ted Cruz (R-Texas), support the USA Freedom Act. Senators Mike Lee (R-Utah) and Patrick Leahy (D-Vermont), who authored the overhaul legislation, said they would not consent to a short-term extension of Section 215 to get past the June 1 deadline.

Others, such as Senate Majority Leader Mitch McConnell (R-Kentucky), Sen. Richard M. Burr (R-North Carolina), chairman of the Senate Intelligence Committee, and Sen. Marco Rubio (R-Florida), want reauthorization with no change.

Still others, including Senators Rand Paul (R-Kentucky) and Ron Wyden (D-Oregon), have threatened to mount a filibuster rather than allow a brief extension of Section 215. They oppose the USA Freedom Act, favoring a stronger bill that would end the metadata collection program.

McConnell has refused to allow the USA Freedom Act to come to the Senate floor for discussion. Some Democrats might agree to a brief extension in exchange for McConnell's agreement to allow the act to be debated.

But any legislation that keeps the bulk metadata collection in place would run afoul of the Court of Appeals decision.

Wyden characterized the Court of Appeals ruling as "a huge step for individual Americans' rights." He added,

> "Now that this program is finally being examined in the sunlight, the executive branch's claims about its legality and effectiveness is crumbling. The president should end mass surveillance immediately. If not, Congress needs to finish the job and finally end this dragnet."

The Privacy and Civil Liberties Oversight Board, as well as a review group appointed by the president, reviewed classified files and concluded that there was no evidence the metadata collection program had ever played a pivotal role in any terrorism investigation.

Congress should take the cue from the Court of Appeals and end the metadata collection program. "If we don't allow Section 215 to sunset," wrote ACLU executive director Anthony Romero, "we risk making permanent a 'new normal' of government surveillance and

extending surveillance programs that haven't yet been – and may never be – disclosed to the public."

Marjorie Cohn is a professor at Thomas Jefferson School of Law, past president of the National Lawyers Guild, and deputy secretary general of the International Association of Democratic Lawyers. Her most recent book is Drones and Targeted Killing: Legal, Moral, and Geopolitical Issues.
