GlobalResearch
Center for Research on Globalization

Mass Surveillance in America: A Timeline of Loosening Laws and Practices

By Cora Currier and Justin Elliott
Global Research, June 09, 2013
ProPublica

Region: USA
Theme: Police State & Civil Rights

by Cora Currier, Justin Elliott and Theodoric Meyer

On Wednesday, the Guardian published a secret court order requiring Verizon to hand over data for all the calls made on its network on an "ongoing, daily basis." Other revelations about surveillance of phone and digital communications have followed.

That the National Security Agency has engaged in such activity isn't entirely new: Since 9/11, we've learned about large-scale surveillance by the spy agency from a patchwork of official statements, classified documents, and anonymously sourced news stories.

Surveillance court created

Sen. Frank Church (D-Idaho) led the investigation.

After a post-Watergate Senate investigation documented abuses of government surveillance, Congress passes the Foreign Intelligence Surveillance Act, or FISA, to regulate how the government can monitor suspected spies or terrorists in the U.S. The law establishes a secret court that issues warrants for electronic surveillance or physical searches of a "foreign power" or "agents of a foreign power" (broadly defined in the law). The government doesn't have to demonstrate probable cause of a crime, just that the "purpose of the surveillance is to obtain foreign intelligence information."

The court's sessions and opinions are classified. The only information we have is a yearly report to the Senate documenting the number of "applications" made by the government. Since 1978, the court has approved thousands of applications – and rejected just 11.

Oct. 2001

Patriot Act passed

President George W. Bush signs the Patriot Act.

In the wake of 9/11, Congress passes the sweeping USA Patriot Act. One provision, section 215, allows the FBI to ask the FISA court to compel the sharing of books, business documents, tax records, library check-out lists – actually, "any tangible thing" – as part of a foreign intelligence or international terrorism investigation. The required material can include purely domestic records.

Oct. 2003

'Vacuum-cleaner surveillance' of the Internet

Mark Klein

AT&T technician Mark Klein discovers what he believes to be newly installed NSA data-mining equipment in a "secret room" at a company facility in San Francisco. Klein, who several years later goes public with his story to support a lawsuit against the company, believes the equipment enables "vacuum-cleaner surveillance of all the data crossing the Internet – whether that be peoples' e-mail, web surfing or any other data."

March 2004

Ashcroft hospital showdown

Attorney General John Ashcroft

In what would become one of the most famous moments of the Bush Administration, presidential aides Andrew Card and Alberto Gonzales show up at the hospital bed of John Ashcroft. Their purpose? To convince the seriously ill attorney general to sign off on the extension of a secret domestic spying program. Ashcroft refuses, believing the warrantless program to be illegal.

The hospital showdown was first reported by the New York Times, but two years later Newsweek provided more detail, describing a program that sounds similar to the one the Guardian revealed this week. The NSA, Newsweek reported citing anonymous sources, collected without court approval vast quantities of phone and email metadata "with cooperation from some of the country's largest telecommunications companies" from "tens of millions of average Americans." The magazine says the program itself began in September 2001 and was shut down in March 2004 after the hospital incident. But Newsweek also raises the possibility that Bush may have found new justification to continue some of the activity.

Dec. 2005

Warrantless wiretapping revealed

Michael Hayden, director of the NSA when the warrantless wiretapping began

The Times, over the objections of the Bush Administration, reveals that since 2002 the government "monitored the international telephone calls and international e-mail messages of hundreds, perhaps thousands, of people inside the United States without warrants." The program involves actually listening in on phone calls and reading emails without seeking permission from the FISA Court.

Jan. 2006

Bush defends wiretapping

President Bush speaks at Kansas State University.

President Bush defends what he calls the “terrorist surveillance program” in a speech in Kansas. He says the program only looks at calls in which one end of the communication is overseas.

March 2006

Patriot Act renewed

The Senate and House pass legislation to renew the USA Patriot Act with broad bipartisan support and President Bush signs it into law. It includes a few new protections for records required to be produced under the controversial section 215.

May 2006

Mass collection of call data revealed

USA Today reports that the NSA has been collecting data since 2001 on phone records of “tens of millions of Americans” through three major phone companies, Verizon, AT&T, and BellSouth (though the companies level of involvement is later disputed.) The data collected does not include content of calls but rather data like phone numbers for analyzing communication patterns.

As with the wiretapping program revealed by the Times, the NSA data collection occurs without warrants, according to USA Today. Unlike the wiretapping program, the NSA data collection was not limited to international communications.

2006

Court authorizes collection of call data

The mass data collection reported by the Guardian this week apparently was first authorized by the FISA court in 2006, though exactly when is not clear. Dianne Feinstein, D-Calif., chairwoman of the Senate intelligence committee, said Thursday, "As far as I know, this is the exact three-month renewal of what has been in place for the past seven years." Similarly, the Washington Post quoted an anonymous "expert in this aspect of the law" who said the document published by the Guardian appears to be a "routine renewal" of an order first issued in 2006.

It's not clear whether these orders represent court approval of the previously warrantless data collection that USA Today described.

Jan. 2007

Bush admin says surveillance now operating with court approval

Attorney General Alberto Gonzalez

Attorney General Alberto Gonzales announces that the FISA court has allowed the government to target international communications that start or end in the U.S., as long as one person is "a member or agent of al Qaeda or an associated terrorist organization." Gonzalez says the government is ending the "terrorist surveillance program," and bringing such cases under FISA approval.

Aug. 2007

Congress expands surveillance powers

The FISA court reportedly changes its stance and puts more limits on the Bush administration's surveillance (the details of the court's move are still not known.) In response, Congress quickly passes, and President Bush signs, a stopgap law, the Protect America Act.

In many cases, the government can now get blanket surveillance warrants without naming specific individuals as targets. To do that, the government needs to show that they're not intentionally targeting people in the U.S., even if domestic communications are swept up in the process.

Sept. 2007

Prism begins

The FBI and the NSA get access to user data from Microsoft under a top-secret program known as Prism, according to an NSA PowerPoint briefing published by the Washington Post and the Guardian this week. In subsequent years, the government reportedly gets data from eight other companies including Apple and Google. “The extent and nature of the data collected from each company varies,” according to the Guardian.

July 2008

Congress renews broader surveillance powers

Congress follows up the Protect America Act with another law, the FISA Amendments Act, extending the government’s expanded spying powers for another four years. The law now approaches the kind of warrantless wiretapping that occurred earlier in Bush administration. Senator Obama votes for the act.

The act also gives immunity to telecom companies for their participation in warrantless wiretapping.

April 2009

NSA ‘overcollects’

The New York Times reports that for several months, the NSA had gotten ahold of domestic communications it wasn’t supposed to. The Times says it was likely the result of “technical problems in the NSA’s ability” to distinguish between domestic and overseas communications. The Justice Department says the problems have been resolved.

Feb. 2010

Controversial Patriot Act provision extended

President Obama

President Obama signs a temporary one-year extension of elements of the Patriot Act that were set to expire — including Section 215, which grants the government broad powers to seize records.

May 2011

Patriot Act renewed, again

The House and Senate pass legislation to extend the overall Patriot Act. President Obama, who is in Europe as the law is set to expire, directs the bill to be signed with an "autopen" machine in his stead. It's the first time in history a U.S. president has done so.

March 2012

Senators warn cryptically of overreach

U.S. Sen. Ron Wyden (D-Ore.)

In a letter to the attorney general, Sens. Ron Wyden, D-Ore., and Mark Udall, D-Colo., write, "We believe most Americans would be stunned to learn the details" of how the government has interpreted Section 215 of the Patriot Act. Because the program is classified, the senators offer no further details.

July 2012

Court finds unconstitutional surveillance

According to a declassified statement by Wyden, the Foreign Intelligence Surveillance Court held on at least one occasion that information collection carried out by the government was unconstitutional. But the details of that episode, including when it happened, have never been revealed.

Dec. 2012

Broad powers again extended

President Obama

Congress extends the FISA Amendments Act another five years, and Obama signs it into law. Sens. Wyden and Jeff Merkley, both Oregon Democrats, offer amendments requiring more disclosure about the law's impact. The proposals fail.

April 2013

Verizon order issued

As the Guardian revealed this week, Foreign Intelligence Surveillance Court Judge Roger Vinson issues a secret court order directing Verizon Business Network Services to turn over "metadata" — including the time, duration and location of phone calls, though not what was said on the calls — to the NSA for all calls over the next three months. Verizon is ordered to deliver the records "on an ongoing daily basis." The Wall Street Journal reports this week that AT&T and Sprint have similar arrangements.

The Verizon order cites Section 215 of the Patriot Act, which allows the FBI to request a court order that requires a business to turn over "any tangible things (including books, records, papers, documents, and other items)" relevant to an international spying or terrorism investigation. In 2012, the government asked for 212 such orders, and the court approved them all.

June 2013

Congress and White House respond

Director of National Intelligence James Clapper

Following the publication of the Guardian's story about the Verizon order, Sens. Feinstein and Saxby Chambliss, R-Ga., the chair and vice of the Senate intelligence committee, hold a news conference to dismiss criticism of the order. "This is nothing particularly new," Chambliss says. "This has been going on for seven years under the auspices of the FISA authority, and every member of the United States Senate has been advised of this."

Director of National Intelligence James Clapper acknowledges the collection of phone metadata but says the information acquired is “subject to strict restrictions on handling” and that “only a very small fraction of the records are ever reviewed.” Clapper alsoissues a statement saying that the collection under the Prism program was justified under the FISA Amendments of 2008, and that it is not “intentionally targeting” any American or person in the U.S.

Statements from the tech companies reportedly taking part in the Prism program variously disavow knowledge of the program and merely state in broad terms they follow the law.

Articles by: Cora Currier and
Justin Elliott