Government Surveillance of Citizens Raises Civil Liberty Concerns

Two revelations about government programs designed to sift through the public's phone calls and social media interaction have raised questions about what the government should be allowed to do in the name of public safety.

Last week the Guardian newspaper reported that the National Security Administration (NSA) has been secretly tracking the phone records of millions of Americans using data supplied by Verizon.

The administration defended the surveillance program, saying that it is lawful and is a "critical tool" to protect national security.

But civil liberties advocates say the program goes too far.

"I was astounded, first of all, to learn for the first time that the government thinks the law allows this, and even more astounded to learn that they were doing it," Kate Martin of the Center for National Security Studies said on the NewsHour.

The person who leaked the information on the surveillance programs revealed himself as Edward Snowden, a 29-year-old employee of defense contractor Booz Allen Hamilton, who had once been assigned to work with the NSA. He says he felt compelled to speak out about what he calls wrongdoing.

"The more you talk about it, the more you are ignored, the more you're told it's not a problem," he said in a video statement to The Guardian newspaper. "Until eventually you realize that these things need to be determined by the public, not by somebody who was simply hired by the government."

Government sifts through Facebook and Google

Meanwhile, the Washington Post revealed that the NSA and FBI have two other spying programs that target American citizens, including one that uses the data of Facebook, Google and Apple, and one that uses information from major credit card companies.

Audio, video, photographs, e-mails, documents and connection logs "enable analysts to track a person's movements and contacts over time," the article explains. "They quite literally can watch your ideas form as you type," an unnamed career intelligence officer told the Post.

The classified PRISM program was established in 2007 and become "the most prolific contributor to the President's Daily Brief," according to the report.

Tech companies have since defended their actions. In an interview with the NewsHour, Google's chief legal officer David Drummond said,"the misimpression is that we're doing some kind of large-scale — or participating in a program that does large-scale surveillance on our users. And that's just not the case."

Instead, he says, "only a tiny, very tiny fraction of [Google] users have ever been subject to one of these requests, national security requests."

Executives at Google, Facebook, Microsoft and Yahoo have all asked the government to lower secrecy around the programs so that they can better explain their role in PRISM.

Spying legal under FISA, says administration

In order to spy on a phone line, the NSA, along with the FBI, CIA and other intelligence agencies, must file a warrant with the Foreign Intelligence Surveillance Court, which reviews the lawfulness of the program. Then, according to Pete Williams of NBC News, the NSA, "goes to the phone companies and says: Every day, pump your data about phone calls into our big government tank — only phone numbers (not names), along with other data about the calls, such as where they came from, how long they lasted, what numbers were dialed, and so on."

The judge who approved this warrant said it was legal because it tracked only the data around the calls, not necessarily the calls themselves. The administration backed this position, saying that the order, “does not allow the government to listen in on anyone’s telephone calls.”

The country’s most secretive court

The courts were set up by the Federal Intelligence Surveillance Act (FISA), which was signed into law in 1978 in the wake of the Watergate scandal as a way to protect American citizens from government spying.

FISA operated mostly without controversy until September 11, 2001, when the Patriot Act expanded the number of judges on the court from seven to 11, and loosened the legal guidelines on who could be monitored.

When it was first reported in 2006 that the Bush administration was wiretapping e-mails and phone calls worldwide in the hunt for terror suspects, then-Senator Barack Obama said it was a — quote — “slippery slope.”
House Speaker Republican John Boehner said it’s now up to President Obama to explain how critical the program is.

Surveillance Under the USA PATRIOT Act

December 10, 2010

What is the USA PATRIOT Act?

Just six weeks after the September 11 attacks, a panicked Congress passed the "USA/Patriot Act," an overnight revision of the nation's surveillance laws that vastly expanded the government's authority to spy on its own citizens, while simultaneously reducing checks and balances on those powers like judicial oversight, public accountability, and the ability to challenge government searches in court.

Why Congress passed the Patriot Act

Most of the changes to surveillance law made by the Patriot Act were part of a longstanding law enforcement wish list that had been previously rejected by Congress, in some cases repeatedly. Congress reversed course because it was bullied into it by the Bush Administration in the frightening weeks after the September 11 attack.

The Senate version of the Patriot Act, which closely resembled the legislation requested by Attorney General John Ashcroft, was sent straight to the floor with no discussion, debate, or hearings. Many Senators complained that they had little chance to read it, much less analyze it, before having to vote. In the House, hearings were held, and a carefully constructed compromise bill emerged from the Judiciary Committee. But then, with no debate or consultation with rank-and-file members, the House leadership threw out the compromise bill and replaced it with legislation that mirrored the Senate version. Neither discussion nor amendments were permitted, and once again members barely had time to read the thick bill before they were forced to cast an up-or-down vote on it. The Bush Administration implied that members who voted against it would be blamed for any further attacks - a powerful threat at a time when the nation was expecting a second attack to come any moment and when reports of new anthrax letters were appearing daily.

Congress and the Administration acted without any careful or systematic effort to determine whether weaknesses in our surveillance laws had contributed to the attacks, or whether the changes they were making would help prevent further attacks. Indeed, many of the act's provisions have nothing at all to do with terrorism.

The Patriot Act increases the government's surveillance powers in four areas

The Patriot Act increases the government's surveillance powers in four areas:

1. Records searches. It expands the government's ability to look at records on an individual's activity being held by third parties. (Section 215)
2. Secret searches. It expands the government's ability to search private property without notice to the owner. (Section 213)
3. Intelligence searches. It expands a narrow exception to the Fourth Amendment that had been created for the collection of foreign intelligence information (Section 218).
4. "Trap and trace" searches. It expands another Fourth Amendment exception for spying that collects "addressing" information about the origin and destination of communications, as opposed to the content (Section 214).

1. Expanded access to personal records held by third parties

One of the most significant provisions of the Patriot Act makes it far easier for the authorities to gain access to records of citizens' activities being held by a third party. At a time when computerization is leading to the creation of more and more such records, Section 215 of the Patriot Act allows the FBI to force anyone at all - including doctors, libraries, bookstores, universities, and Internet service providers - to turn over records on their clients or customers.

Unchecked power

The result is unchecked government power to rifle through individuals' financial records, medical histories, Internet usage, bookstore purchases, library usage, travel patterns, or any other activity that leaves a record. Making matters worse:

- The government no longer has to show evidence that the subjects of search orders are an "agent of a foreign power," a requirement that previously protected Americans against abuse of this authority.

- The FBI does not even have to show a reasonable suspicion that the records are related to criminal activity, much less the requirement for "probable cause" that is listed in the Fourth Amendment to the Constitution. All the government needs to do is make the broad assertion that the request is related to an ongoing terrorism or foreign intelligence investigation.
- Judicial oversight of these new powers is essentially non-existent. The government must only certify to a judge - with no need for evidence or proof - that such a search meets the statute's broad criteria, and the judge does not even have the authority to reject the application.
- Surveillance orders can be based in part on a person's First Amendment activities, such as the books they read, the Web sites they visit, or a letter to the editor they have written.
- A person or organization forced to turn over records is prohibited from disclosing the search to anyone. As a result of this gag order, the subjects of surveillance never even find out that their personal records have been examined by the government. That undercuts an important check and balance on this power: the ability of individuals to challenge illegitimate searches.

Why the Patriot Act's expansion of records searches is unconstitutional
Section 215 of the Patriot Act violates the Constitution in several ways. It:

- Violates the Fourth Amendment, which says the government cannot conduct a search without obtaining a warrant and showing probable cause to believe that the person has committed or will commit a crime.
- Violates the First Amendment's guarantee of free speech by prohibiting the recipients of search orders from telling others about those orders, even where there is no real need for secrecy.
- Violates the First Amendment by effectively authorizing the FBI to launch investigations of American citizens in part for exercising their freedom of speech.
- Violates the Fourth Amendmentby failing to provide notice - even after the fact - to persons whose privacy has been compromised. Notice is also a key element of due process, which is guaranteed by the Fifth Amendment.

2. More secret searches

For centuries, common law has required that the government can't go into your property without telling you, and must therefore give you notice before it executes a search. That "knock and announce" principle has long been recognized as a part of the Fourth Amendment to the Constitution.

The Patriot Act, however, unconstitutionally amends the Federal Rules of Criminal Procedure to allow the government to conduct searches without notifying the subjects, at least until long after the search has been executed. This means that the government can enter a house, apartment or office with a search warrant when the occupants are away, search through their property, take photographs, and in some cases even seize property - and not tell them until later.

Notice is a crucial check on the government's power because it forces the authorities to operate in the open, and allows the subject of searches to protect their Fourth Amendment rights. For example, it allows them to point out irregularities in a warrant, such as the fact that the police are at the wrong address, or that the scope of the warrant is being exceeded (for example, by rifling through dresser drawers in a search for a stolen car). Search warrants often contain limits on what may be searched, but when the searching officers have complete and unsupervised discretion over a search, a property owner cannot defend his or her rights.

Finally, this new "sneak and peek" power can be applied as part of normal criminal investigations; it has nothing to do with fighting terrorism or collecting foreign intelligence.

3. Expansion of the intelligence exception in wiretap law

Under the Patriot Act, the FBI can secretly conduct a physical search or wiretap on American citizens to obtain evidence of crime without proving probable cause, as the Fourth Amendment explicitly requires.

A 1978 law called the Foreign Intelligence Surveillance Act (FISA) created an exception to the Fourth Amendment's requirement for probable cause when the purpose of a wiretap or search was to gather foreign intelligence. The rationale was that since the search was not conducted for the purpose of gathering evidence to put someone on trial, the standards could be loosened. In a stark demonstration of why it can be dangerous to create exceptions to fundamental rights, however, the Patriot Act expanded this once-narrow exception to cover wiretaps and searches that DO collect evidence for regular domestic criminal cases. FISA previously allowed searches only if the primary purpose was to gather foreign intelligence. But the Patriot Act changes the law to allow searches when "a significant purpose" is intelligence. That lets the government circumvent the Constitution's probable cause requirement even when its main goal is ordinary law enforcement.

The eagerness of many in law enforcement to dispense with the requirements of the Fourth Amendment was revealed in August 2002 by the secret court that oversees domestic intelligence spying (the "FISA Court"). Making public one of its opinions for the first time in history, the court revealed that it had rejected an attempt by the Bush Administration to allow criminal prosecutors to use intelligence warrants to evade the Fourth Amendment entirely. The court also noted that agents applying for warrants had regularly filed false and misleading information. That opinion is now on appeal.

4. Expansion of the "pen register" exception in wiretap law

Another exception to the normal requirement for probable cause in wiretap law is also expanded by the Patriot Act. Years ago, when the law governing telephone wiretaps was written, a distinction was created between two types of surveillance. The first allows surveillance of the content or meaning of a communication, and the second only allows monitoring of the transactional or addressing information attached to a communication. It is like the difference between reading the address printed on the outside of a letter, and reading the letter inside, or listening to a phone conversation and merely recording the phone numbers dialed and received.

Wiretaps limited to transactional or addressing information are known as "Pen register/trap and trace" searches (for the devices that were used on telephones to collect telephone numbers). The requirements for getting a PR/TT warrant are essentially non-existent: the FBI need not show probable cause or even reasonable suspicion of criminal activity. It must only certify to a judge - without having to prove it - that such a warrant would be "relevant" to an ongoing criminal investigation. And the judge does not even have the authority to reject the application.

The Patriot Act broadens the pen register exception in two ways:

"Nationwide" pen register warrants
Under the Patriot Act PR/TT orders issued by a judge are no longer valid only in that judge's jurisdiction, but can be made valid anywhere in the United States. This "nationwide service" further marginalizes the role of the judiciary, because a judge cannot meaningfully monitor the extent to which his or her order is being used. In addition, this provision authorizes the equivalent of a blank warrant: the court issues the order, and the law enforcement agent fills in the places to be searched. That is a direct violation of the Fourth Amendment's explicit requirement that warrants be written "particularly describing the place to be searched."

Pen register searches applied to the Internet
The Patriot Act applies the distinction between transactional and content-oriented wiretaps to the Internet. The problem is that it takes the weak standards for access to transactional data and applies them to communications that are far more than addresses. On an e-mail message, for example, law enforcement has interpreted the "header" of a message to be transactional information

accessible with a PR/TT warrant. But in addition to routing information, e-mail headers include the subject line, which is part of the substance of a communication - on a letter, for example, it would clearly be inside the envelope.

The government also argues that the transactional data for Web surfing is a list of the URLs or Web site addresses that a person visits. For example, it might record the fact that they visited "www.aclu.org" at 1:15 in the afternoon, and then skipped over to "www.fbi.gov" at 1:30. This claim that URLs are just addressing data breaks down in two different ways:

- Web addresses are rich and revealing content. The URLs or "addresses" of the Web pages we read are not really addresses, they are the titles of documents that we download from the Internet. When we "visit" a Web page what we are really doing is downloading that page from the Internet onto our computer, where it is displayed. Therefore, the list of URLs that we visit during a Web session is really a list of the documents we have downloaded - no different from a list of electronic books we might have purchased online. That is much richer information than a simple list of the people we have communicated with; it is intimate information that reveals who we are and what we are thinking about - much more like the content of a phone call than the number dialed. After all, it is often said that reading is a "conversation" with the author.
- Web addresses contain communications sent by a surfer. URLs themselves often have content embedded within them. A search on the Google search engine, for example, creates a page with a custom-generated URL that contains material that is clearly private content, such as: http://www.google.com/search?hl=en&lr=&ie=UTF-8&oe=UTF-8&q=sexual+orient...

Similarly, if I fill out an online form - to purchase goods or register my preferences, for example - those products and preferences will often be identified in the resulting URL.