Snooping highlights lower privacy standards for email, cellphones

May 29 2013, by Cornelius Frolik

Law enforcement can potentially spy on the American people without their knowledge or an oversight from a judge, thanks to antiquated laws that privacy advocates say haven't kept pace with technology advances.

"We haven't had a wide-scale change in our privacy laws since the 1980s, and imagine where we were with technology back then compared to today," said Mike Brickner, director of communications and public policy for the American Civil Liberties Union of Ohio.

Government agencies don't need search warrants in many cases to obtain people's private emails, electronic messages and cellphone records. Instead, they can acquire the records through subpoenas, which require less strict standards of evidence.

Law enforcement is increasingly using its subpoena power on social media providers like Google to obtain information on users during criminal investigations. The reporting requirements are such that average Americans may never know they are being snooped on unless the surveillance results in criminal charges.

The U.S. Department of Justice used subpoenas to secretly seize phone records of editors and reporters from the Associated Press, allegedly as part of a leak investigation, without first getting a warrant from a judge. Critics said the amount of information the government collected was "harassingly broad" and unconstitutional.

"I am confident our members are outraged and concerned about the targeting of journalists by the Justice Department without prior knowledge, advance warning or the approval of a judge," said Dennis Hetzel, executive director of the Ohio Newspaper Association.

The Justice Department also sought emails in a leak investigation involving Fox News reporter James Rosen, though in that case the department filed an affidavit for a search warrant, which does require judicial approval.

Information obtained from subpoenas has helped local authorities catch dangerous criminals. Cellular records helped prove that one murder suspect's alibi was a lie, and Internet subscriber records have helped identify sex offenders.

But privacy advocates said the government too easily can access many personal communications and other private information without sufficient probable cause. They are calling on Congress to stop "warrantless snooping" by updating digital privacy laws to account for the rise of cellphones, social media and email.

Warrants are necessary to wiretap phones and listen in on conversations as part of the Fourth Amendment's protections against unreasonable searches and seizures. Authorities usually also need a warrant to seize letters sent through the mail.

But different rules apply to digital communications, even though emails and texts have replaced letters as the primary forms of written communication.

Under the 1986 Electronic Communications Privacy Act, the government does not need a warrant to obtain emails and electronic messages that are 180 days old or that have been opened, experts said.

"The statute says that only a subpoena is necessary," said Paul Rosenzweig, a visiting fellow with the Heritage Foundation, a conservative think tank in Washington, D.C.

Subpoenas have become a go-to investigative tool because they can be written out in a prosecutor's office without anyone's review, Rosenzweig said.

"It is very rare that investigators will jump through the hoops that you need to go through to get a wiretap order - which requires a fairly high standard - when they can get email and other stored records much more easily," said Julian Sanchez, research fellow with the Washington-based Cato Institute, which seeks to advance limited government and individual liberty. "The records are subject to an almost trivial standard of evidence, which is relevance to an investigation."

How the information is used depends on what the government finds.

"If your email is lawfully acquired, anything disclosed in the email can be used by the government," Rosenzweig said. "If they solicit your emails because they think you are a drug dealer, and it turns out they are wrong but you have emails about undisclosed income you have in the Cayman Islands, they will take copies and send them to the IRS."

It is unknown how often government agencies obtain personal emails or information about email users as part of investigations.

Only a small fraction of government requests for electronic records is subject to reporting requirements, experts said. As a result, the scope of the snooping is largely a mystery.

But in the last six months of 2012, Google - which offers email, video chat and instant messaging through its Gmail service - said it received

8,438 requests for user information from U.S. law enforcement agencies. About 70 percent of requests were subpoenas, while about 22 percent were probable-cause warrants.

Google, Microsoft and some other major companies said they will not release the contents of subscribers' emails and electronic messages unless they receive a warrant. Google, however, reported producing other noncontent subscriber information in almost 90 percent of the law enforcement requests.

Microsoft - which owns the Outlook.com email service, formerly known as Hotmail - said last year it provided subscriber and transactional data in two-thirds of the 11,000 requests from U.S. law enforcement it received. In 14 percent of the requests, Microsoft produced the content of emails.

Transactional information can include who sent and received messages, when they were delivered and possibly the location where they were transmitted. Such information is invaluable in many law enforcement investigations.

Prosecutors in New York subpoenaed Twitter for tweets, IP addresses and other information of an Occupy Wall Street protester who was charged with disorderly conduct for marching on the roadway of the Brooklyn Bridge.

Twitter fought the subpoena in court but eventually turned the information over, said Thaddeus Hoffmeister, law professor with the University of Dayton School of Law.

"Twitter fought them a little, but generally social media providers roll over and give your stuff up," he said. "They don't want the government to step in and regulate them more heavily."

Subpoenas don't always produce the contents of emails, but they can reveal other information useful to law enforcement.

The Ohio Bureau of Criminal Identification subpoenaed AT&T Internet Services to identify a Beavercreek, Ohio, man who owned an IP address associated with child pornography.

The man's home was searched, and he was arrested and convicted of multiple felonies.

Government agencies also can acquire cellphone and text message records through subpoenas, which can include geolocation data showing where the phones were at certain times.

That, too, can be a case-solver for police.

In 2010, Trotwood, Ohio, police subpoenaed records from Cincinnati Bell that showed a murder suspect had lied about his whereabouts at the time of the homicide.

The suspect claimed to be in another town when the victim was killed in Trotwood.

But wireless records showed his cellphone signals were transmitted by towers near Trotwood around the time of the killing.

Cincinnati Bell said it does not know how often it receives subpoenas and other requests for information. But the company said it follows strict procedures when responding to the requests.

"Requests from law enforcement or subpoenas by the courts are handled by the office of our corporate counsel to ensure that we're complying with all applicable laws in this area," said Angela Ginty, spokeswoman

for Cincinnati Bell.

In 2011, federal, state and local law enforcement agencies made about 1.3 million requests to some of the largest U.S. cellular providers for the wireless device records of customers, according to information obtained and released last year by Rep. Edward Markey, D-Mass.

The requests from law enforcement asked for information including geolocation, call records, content of text messages and wiretaps.

AT&T received 131,400 subpoenas for cellular records in 2011, more than double what it received in 2008, according to a letter from the company. It also received 49,700 warrants and orders in 2011.

Many U.S. law enforcement agencies are tracking cellphones without warrants and demonstrating probable cause, according to an ACLU analysis of documents from about 250 police departments.

Additionally, people whose phone and email records are obtained and scrutinized by the government will likely not find out about the intrusion if they are never charged with a crime, privacy experts said. The law does not require that the government notify subscribers of third-party services that their records were put under the microscope.

John Murphy, director of the Ohio Prosecuting Attorneys Association, said evidence in a criminal case obtained through subpoenas can be challenged in court - a protection for those who believe their privacy has been violated.

"If the person (whose information) is being subpoenaed thinks the subpoena is overbroad and asks for things it shouldn't be asking for, they can file a motion to quash, which goes before the court," Murphy said.

But privacy advocacy groups said more protections are needed.

The proposed Electronic Communications Privacy Act Amendments Act of 2013, now pending in Congress, would update the 1986 law by requiring the government to obtain a search warrant to get the contents of emails, texts, social media posts and other communications stored with third-party service providers. The legislation, which has bipartisan support, would also eliminate the 180-day rule on electronic messages, and require the government to notify people when it seizes their electronic communications.

Domestic spying and intelligence-gathering activities that do not require a warrant are rife with potential for abuse, said Brickner of the ACLU of Ohio.

"Once you can justify wrongly surveilling one group of people, it is very easy to do it with other groups that come along," he said. "We need to change some of these laws and reverse this tide, otherwise we are just going to hear about these outrages and hear about the press being surveilled and political groups being wrongly targeted."

PRIVACY V. INVESTIGATIVE AUTHORITY

Companies like Google and YouTube have policies governing the type of information they will reveal to investigators under a subpoena: subscriber registration information, sign-in IP addresses and associated time stamps, for example. Subpoenas can be used in both civil and criminal cases.

If subpoenaed, Google will release the following information:

-Name

-Account creation information

-Associated email addresses

-Phone number