Is Big Data turning government into 'Big Brother?'

MICHAEL LIEDTKE - AP Technology Writer - Associated Press

With every phone call they make and every Web excursion they take, people are leaving a digital trail of revealing data that can be tracked by profit-seeking companies and terrorist-hunting government officials.

The revelations that the National Security Agency is perusing millions of U.S. customer phone records at Verizon Communications and snooping on the digital communications stored by nine major Internet services illustrate how aggressively personal data is being collected and analyzed.

Verizon is handing over so-called metadata, excerpts from millions of U.S. customer records, to the NSA under an order issued by the secretive Foreign Intelligence Surveillance Court, according to a report in the British newspaper The Guardian. The report was confirmed Thursday by Sen. Dianne Feinstein, D-Calif., who chairs the Senate Intelligence Committee.

Former NSA employee William Binney told the Associated Press that he estimates the agency collects records on 3 billion phone calls each day.

The NSA and FBI appear to be casting an even wider net under a clandestine program code-named "PRISM" that came to light in a story posted late Thursday by The Washington Post. PRISM gives the U.S. government access to email, documents, audio, video, photographs and other data that people entrust to some of the world's best known companies, according to The Washington Post. The newspaper said it reviewed a confidential roster of companies and services participating in PRISM. The companies included AOL Inc., Apple Inc., Facebook Inc., Google Inc., Microsoft Corp., Yahoo Inc., Skype, YouTube and Paltalk.

In statements, Apple, Facebook, Google, Microsoft and Yahoo said they only provide the government with user data required under the law. (Google runs YouTube and Microsoft owns Skype.) AOL and Paltalk didn't immediately respond to inquiries from The Associated Press.

The NSA isn't getting customer names or the content of phone conversations under the Verizon court order, but that doesn't mean the information can't be tied to other data coming in through the PRISM program to look into people's lives, according to experts.

Like pieces of a puzzle, the bits and bytes left behind from citizens' electronic interactions can be cobbled together to draw conclusions about their habits, friendships and preferences using data-mining formulas and increasingly powerful computers.

It's all part of a phenomenon known as a "Big Data," a catchphrase increasingly used to describe the science of analyzing the vast amount of information collected through mobile devices, Web browsers and check-out stands. Analysts use powerful computers to detect trends and create digital dossiers about people.

The Obama administration and lawmakers privy to the NSA's surveillance aren't saying anything about the collection of the Verizon customers' records beyond that it's in the interest of national security. The sweeping court order covers the Verizon records of every mobile and landline phone call from April 25 through July 19, according to The Guardian.

It's likely the Verizon phone records are being matched with an even broader set of data, said Forrester Research analyst Fatemeh Khatibloo.

"My sense is they are looking for network patterns," she said. "They are looking for who is connected to whom and whether they can put any timelines together. They are also probably trying to identify locations where people are calling from."

Under the court order, the Verizon records include the duration of every call and the locations of mobile calls, according to The Guardian.

The location information is particularly valuable for cloak-and-dagger operations like the one the NSA is running, said Cindy Cohn, a legal director for the Electronic Frontier Foundation, a digital rights group that has been fighting the government's collection of personal phone records since 2006. The foundation is currently suing over the government's collection of U.S. citizens' communications in a case that dates back to the administration of President George W. Bush.

"It's incredibly invasive," Cohn said. "This is a consequence of the fact that we have so many third parties that have accumulated significant information about our everyday lives."

It's such a rich vein of information that U.S. companies and other organizations now spend more than $2 billion each year to obtain third-party data about individuals, according to Forrester Research. The data helps businesses target potential customers. Much of this information is sold by so-called data brokers such as Acxiom Corp., a Little Rock, Ark. company that maintains extensive files about the online and offline activities of more than 500 million consumers worldwide.

The digital floodgates have opened during the past decade as the convenience and allure of the Internet —and sleek smartphones— have made it easier and more enjoyable for people to stay connected wherever they go.

"I don't think there has been a sea change in analytical methods as much as there has been a change in the volume, velocity and variety of information and the computing power to process it all," said Gartner analyst Douglas Laney.

In a sign of the NSA's determination to vacuum up as much data as possible, the

agency has built a data center in Bluffdale, Utah that is five times larger than the U.S. Capitol —all to sift through Big Data. The $2 billion center has fed perceptions that some factions of the U.S. government are determined to build a database of all phone calls, Internet searches and emails under the guise of national security. The Washington Post's disclosure that both the NSA and FBI have the ability to burrow into computers of major Internet services will likely heighten fears that U.S. government's Big Data is creating something akin to the ever-watchful Big Brother in George Orwell's "1984" novel.

"The fact that the government can tell all the phone carriers and Internet service providers to hand over all this data sort of gives them carte blanche to build profiles of people they are targeting in a very different way than any company can," Khatibloo said.

In most instances, Internet companies such as Google Inc., Facebook Inc. and Yahoo Inc. are taking what they learn from search requests, clicks on "like" buttons, Web surfing activity and location tracking on mobile devices to figure out what each of their users like and divine where they are. It's all in aid of showing users ads about products likely to pique their interest at the right time. The companies defend this kind of data mining as a consumer benefit.

Google is trying to take things a step further. It is honing its data analysis and search formulas in an attempt to anticipate what an individual might be wondering about or wanting.

Other Internet companies also use Big Data to improve their services. Video subscription service Netflix takes what it learns from each viewer's preferences to recommend movies and TV shows. Amazon.com Inc. does something similar when it highlights specific products to different shoppers visiting its site.

The federal government has the potential to know even more about people because it controls the world's biggest data bank, said David Vladeck, a Georgetown University law professor who recently stepped down as the Federal Trade Commission's consumer protection director.

Before leaving the FTC last year, Vladeck opened an inquiry into the practices of Acxiom and other data brokers because he feared that information was being misinterpreted in ways that unfairly stereotyped people. For instance, someone might be classified as a potential health risk just because they bought products linked to an increased chance of heart attack. The FTC inquiry into data brokers is still open.

"We had real concerns about the reliability of the data and unfair treatment by algorithm," Vladeck said.

Vladeck stressed he had no reason to believe that the NSA is misinterpreting the data it collects about private citizens. He finds some comfort in The Guardian report that said the Verizon order had been signed by Foreign Intelligence Surveillance Court Judge Ronald Vinson.

The NSA "differs from a commercial enterprise in the sense that there are checks in the judicial system and in Congress," Vladeck said. "If you believe in the way our government is supposed to work, then you should have some faith that those checks are meaningful. If you are skeptical about government, then you probably don't think that kind of oversight means anything."

Source URL (retrieved on *03/10/2014 - 6:34am*):
http://www.ecnmag.com/news/2013/06/big-data-turning-government-big-brother