Secret to Prism program: Even bigger data seizure

June 15 2013, by Anne Flaherty

In this June 10, 2013 file photo, President Barack Obama speaks in the East Room of the White House in Washington. Wondering what the U.S. government might know about your phone calls and online life? And whether all of this really helps find terrorists? Good luck finding solid answers. Americans trying to wrap their minds around two giant surveillance programs are confronted with a mishmash of leaks, changing claims and secrecy. Congress members complain their constituents are baffled _ and many lawmakers admit they are, too. (AP Photo/Carolyn Kaster, File)

In the months and early years after the Sept. 11, 2001, terrorist attacks, FBI agents began showing up at Microsoft Corp. more frequently than before, armed with court orders demanding information on customers.

Around the world, government spies and eavesdroppers were tracking the email and Internet addresses used by suspected terrorists. Often, those trails led to the world's largest software company and, at the time, largest email provider.

The agents wanted email archives, account information, practically everything, and quickly. Engineers compiled the data, sometimes by hand, and delivered it to the government.

Often there was no easy way to tell if the information belonged to foreigners or Americans. So much data was changing hands that one former Microsoft employee recalls that the engineers were anxious about whether the company should cooperate.

Inside Microsoft, some called it "Hoovering"—not after the vacuum cleaner, but after J. Edgar Hoover, the first FBI director, who gathered dirt on countless Americans.

This frenetic, manual process was the forerunner to Prism, the recently revealed highly classified National Security Agency program that seizes records from Internet companies. As laws changed and technology improved, the government and industry moved toward a streamlined, electronic process, which required less time from the companies and provided the government data in a more standard format.

The revelation of Prism this month by the Washington Post and Guardian newspapers has touched off the latest round in a decade-long debate over what limits to impose on government eavesdropping, which the Obama administration says is essential to keep the U.S. safe.

But interviews with more than a dozen current and former government and technology officials and outside experts show that, while Prism has attracted the recent attention, the program actually is a relatively small part of a much more expansive and intrusive eavesdropping effort.

Americans who disapprove of the government reading their emails have more to worry about from a different and larger NSA effort that snatches data as it passes through the fiber optic cables that make up the Internet's backbone. That program, which has been known for years, copies Internet traffic as it enters and leaves the United States, then routes it to the NSA for analysis.

Whether by clever choice or coincidence, Prism appears to do what its name suggests. Like a triangular piece of glass, Prism takes large beams of data and helps the government find discrete, manageable strands of information.

The fact that it is productive is not surprising; documents show it is one of the major sources for what ends up in the president's daily briefing. Prism makes sense of the cacophony of the Internet's raw feed. It provides the government with names, addresses, conversation histories and entire archives of email inboxes.

Many of the people interviewed for this report insisted on anonymity because they were not authorized to publicly discuss a classified, continuing effort. But those interviews, along with public statements and the few public documents available, show there are two vital components to Prism's success.

The first is how the government works closely with the companies that keep people perpetually connected to each other and the world. That story line has attracted the most attention so far.

The second and far murkier one is how Prism fits into a larger U.S. wiretapping program in place for years.

—–

Deep in the oceans, hundreds of cables carry much of the world's phone and Internet traffic. Since at least the early 1970s, the NSA has been tapping foreign cables. It doesn't need permission. That's its job.

But Internet data doesn't care about borders. Send an email from Pakistan to Afghanistan and it might pass through a mail server in the United States, the same computer that handles messages to and from Americans. The NSA is prohibited from spying on Americans or anyone inside the United States. That's the FBI's job and it requires a warrant.

Despite that prohibition, shortly after the Sept. 11 terrorist attacks, President George W. Bush secretly authorized the NSA to plug into the fiber optic cables that enter and leave the United States, knowing it would give the government unprecedented, warrantless access to Americans' private conversations.

Tapping into those cables allows the NSA access to monitor emails, telephone calls, video chats, websites, bank transactions and more. It takes powerful computers to decrypt, store and analyze all this information, but the information is all there, zipping by at the speed of light.

"You have to assume everything is being collected," said Bruce Schneier, who has been studying and writing about cryptography and computer security for two decades.

The New York Times disclosed the existence of this effort in 2005. In 2006, former AT&T technician Mark Klein revealed that the company had allowed the NSA to install a computer at its San Francisco switching center, a spot where fiber optic cables enter the U.S.

What followed was the most significant debate over domestic surveillance since the 1975 Church Committee, a special Senate committee led by Sen. Frank Church of Idaho, reined in the CIA and FBI for spying on Americans.

Unlike the recent debate over Prism, however, there were no visual aids, no easy-to-follow charts explaining that the government was sweeping up millions of emails and listening to phone calls of people accused of no wrongdoing.

The Bush administration called it the "Terrorist Surveillance Program" and said it was keeping the United States safe.

"This program has produced intelligence for us that has been very valuable in the global war on terror, both in terms of saving lives and breaking up plots directed at the United States," Vice President Dick Cheney said at the time.

The government has said it minimizes all conversations and emails involving Americans. Exactly what that means remains classified. But former U.S. officials familiar with the process say it allows the government to keep the information as long as it is labeled as belonging to an American and stored in a special, restricted part of a computer.

That means Americans' personal emails can live in government computers, but analysts can't access, read or listen to them unless the emails become relevant to a national security investigation.

The government doesn't automatically delete the data, officials said, because an email or phone conversation that seems innocuous today might be significant a year from now.

What's unclear to the public is how long the government keeps the data. That is significant because the U.S. someday will have a new enemy. Two decades from now, the government could have a trove of American emails and phone records it can tap to investigative whatever Congress declares a threat to national security.

Gen. Keith Alexander, Director of the National Security Agency, leaves a Senate Intelligence Committee meeting regarding NSA programs, in Washington, Thursday, June 13, 2013. (AP Photo/Jacquelyn Martin)

The Bush administration shut down its warrantless wiretapping program in 2007 but endorsed a new law, the Protect America Act, which allowed the wiretapping to continue with changes: The NSA generally would have to explain its techniques and targets to a secret court in Washington, but individual warrants would not be required.

Congress approved it, with Illinois Sen. Barack Obama, in the midst of a campaign for president, voting against it.

"This administration also puts forward a false choice between the liberties we cherish and the security we provide," Obama said in a speech two days before that vote. "I will provide our intelligence and law enforcement agencies with the tools they need to track and take out the terrorists without undermining our Constitution and our freedom."

___

When the Protect America Act made warrantless wiretapping legal, lawyers and executives at major technology companies knew what was about to happen.

One expert in national security law, who is directly familiar with how Internet companies dealt with the government during that period, recalls conversations in which technology officials worried aloud that the government would trample on Americans' constitutional right against unlawful searches, and that the companies would be called on to help.

The logistics were about to get daunting, too.

For years, the companies had been handling requests from the FBI. Now Congress had given the NSA the authority to take information without warrants. Though the companies didn't know it, the passage of the Protect America Act gave birth to a top-secret NSA program, officially called US-98XN.

It was known as Prism. Though many details are still unknown, it worked like this:

Every year, the attorney general and the director of national intelligence spell out in a classified document how the government plans to gather intelligence on foreigners overseas.

By law, the certification can be broad. The government isn't required to identify specific targets or places.

A federal judge, in a secret order, approves the plan.

With that, the government can issue "directives" to Internet companies to turn over information.

While the court provides the government with broad authority to seize records, the directives themselves typically are specific, said one former associate general counsel at a major Internet company. They identify a specific target or groups of targets. Other company officials recall similar experiences.

All adamantly denied turning over the kind of broad swaths of data that many people believed when the Prism documents were first released.

"We only ever comply with orders for requests about specific accounts or identifiers," Microsoft said in a statement.

Facebook said it received between 9,000 and 10,000 requests for data from all government agencies in the second half of last year. The social media company said fewer than 19,000 users were targeted.

How many of those were related to national security is unclear, and likely classified. The numbers suggest each request typically related to one or two people, not a vast range of users.

Tech company officials were unaware there was a program named Prism. Even former law enforcement and counterterrorism officials who were on the job when the program went live and were aware of its capabilities said this past week that they didn't know what it was called.

What the NSA called Prism, the companies knew as a streamlined system that automated and simplified the "Hoovering" from years earlier, the former assistant general counsel said. The companies, he said, wanted to reduce their workload. The government wanted the data in a structured, consistent format that was easy to search.

Any company in the communications business can expect a visit, said Mike Janke, CEO of Silent Circle, a company that advertises software for secure, encrypted conversations. The government is eager to find easy ways around security.

In this June 6, 2013, photo, Sen. Lindsey Graham, R-S.C., right, joined by Sen. Susan Collins, R-Maine, left, addresses Attorney General Eric Holder as he testifies at a Senate Appropriations subcommittee as lawmakers examine the budget for the Justice Department, on Capitol Hill in Washington. Revelations of massive government collections of Americans' phone and email records have reinvigorated an odd-couple political alliance of the far left and right. "This is a marginal national security group within our party," Graham said of those who call the government snooping unwarranted or unconstitutional. "I just don't see how anybody gets elected as a Republican" by running to the "left of Obama on national security," said Graham, one of the Senate's most hawkish members. (AP Photo/J. Scott Applewhite)

"They do this every two to three years," said Janke, who said government agents have approached his company but left empty-handed because his computer servers store little information. "They ask for the moon."

That often creates tension between the government and a technology industry with a reputation for having a civil libertarian bent. Companies occasionally argue to limit what the government takes. Yahoo even went to court and lost in a classified ruling in 2008, The New York Times reported Friday.

"The notion that Yahoo gives any federal agency vast or unfettered access to our users' records is categorically false," Ron Bell, the company's general counsel, said recently.

Under Prism, the delivery process varied by company.

Google, for instance, says it makes secure file transfers. Others use contractors or have set up stand-alone systems. Some have set up user interfaces making it easier for the government, according to a security expert familiar with the process.

Every company involved denied the most sensational assertion in the Prism documents: that the NSA pulled data "directly from the servers" of Microsoft, Yahoo, Google, Facebook, AOL and more.

Technology experts and a former government official say that phrasing, taken from a PowerPoint slide describing the program, was likely meant to differentiate Prism's neatly organized, company-provided data from the unstructured information snatched out of the Internet's major pipelines.

In a slide made public by the Post and Guardian, NSA analysts were encouraged to use data coming from both Prism and from the fiber-optic cables.

Prism, as its name suggests, helps narrow and focus the stream. If eavesdroppers spot a suspicious email among the torrent of data pouring into the United States, analysts can use information from Internet companies to pinpoint the user.

With Prism, the government gets a user's entire email inbox. Every email, including contacts with American citizens, becomes government property.

Once the NSA has an inbox, it can search its huge archives for information about everyone with whom the target communicated. All those people can be investigated, too.

That's one example of how emails belonging to Americans can become swept up in the hunt.

In that way, Prism helps justify specific, potentially personal searches. But it's the broader operation on the Internet fiber optics cables that actually captures the data, experts agree.

"I'm much more frightened and concerned about real-time monitoring on the Internet backbone," said Wolf Ruzicka, CEO of EastBanc Technologies, a Washington software company. "I cannot think of anything, outside of a face-to-face conversation, that they could not have access to."

One unanswered question, according to a former technology executive at one of the companies involved, is whether the government can use the data from Prism to work backward.

For example, not every company archives instant message conversations, chat room exchanges or videoconferences. But if Prism provided general details, known as metadata, about when a user began chatting, could the government "rewind" its copy of the global Internet stream, find the conversation and replay it in full?

That would take enormous computing, storage and code-breaking power. It's possible the NSA could use supercomputers to decrypt some transmissions, but it's unlikely it would have the ability to do that in volume. In other words, it would help to know what messages to zero in on.

Whether the government has that power and whether it uses Prism this way remains a closely guarded secret.

___

A few months after Obama took office in 2009, the surveillance debate reignited in Congress because the NSA had crossed the line. Eavesdroppers, it turned out, had been using their warrantless wiretap authority to intercept far more emails and phone calls of Americans than they were supposed to.

Obama, no longer opposed to the wiretapping, made unspecified changes to the process. The government said the problems were fixed.

"I came in with a healthy skepticism about these programs," Obama explained recently. "My team evaluated them. We scrubbed them thoroughly. We actually expanded some of the oversight, increased some of the safeguards."

Years after decrying Bush for it, Obama said Americans did have to make tough choices in the name of safety.

"You can't have 100 percent security and also then have 100 percent privacy and zero inconvenience," the president said.

Obama's administration, echoing his predecessor's, credited the surveillance with disrupting several terrorist attacks. Leading figures from the Bush administration who endured criticism during Obama's candidacy have applauded the president for keeping the surveillance intact.

Jason Weinstein, who recently left the Justice Department as head of its cybercrime and intellectual property section, said it's no surprise Obama continued the eavesdropping.

"You can't expect a president to not use a legal tool that Congress has given him to protect the country," he said. "So, Congress has given him the tool. The president's using it. And the courts are saying 'The way you're using it is OK.' That's checks and balances at work."

Schneier, the author and security expert, said it doesn't really matter how Prism works, technically. Just assume the government collects everything, he said.

He said it doesn't matter what the government and the companies say, either. It's spycraft, after all.

"Everyone is playing word games," he said. "No one is telling the truth."

Citation: Secret to Prism program: Even bigger data seizure (2013, June 15) retrieved 15 July 2024 from https://phys.org/news/2013-06-secret-prism-bigger-seizure.html