wsj.com

New Details Show Broader NSA Surveillance Reach

Siobhan Gorman and Jennifer Valentino-DeVries

14-18 minutes

WASHINGTON—The National Security Agency—which possesses only limited legal authority to spy on U.S. citizens—has built a surveillance network that covers more Americans' Internet communications than officials have publicly disclosed, current and former officials say.

The system has the capacity to reach roughly 75% of all U.S. Internet traffic in the hunt for foreign intelligence, including a wide array of communications by foreigners and Americans. In some cases, it retains the written content of emails sent between citizens within the U.S. and also filters domestic phone calls made with Internet technology, these people say.

The NSA's filtering, carried out with telecom companies, is designed to look for communications that either originate or end abroad, or are entirely foreign but happen to be passing through the U.S. But officials say the system's broad reach makes it more likely that purely domestic communications will be incidentally intercepted and collected in the hunt for foreign

ones.

The programs, code-named Blarney, Fairview, Oakstar, Lithium and Stormbrew, among others, filter and gather information at major telecommunications companies. Blarney, for instance, was established with AT&T Inc., former officials say. AT&T declined to comment.

This filtering takes place at more than a dozen locations at major Internet junctions in the U.S., officials say. Previously, any NSA filtering of this kind was largely believed to be happening near points where undersea or other foreign cables enter the country.

Details of these surveillance programs were gathered from interviews with current and former intelligence and government officials and people from companies that help build or operate the systems, or provide data. Most have direct knowledge of the work.

The NSA defends its practices as legal and respectful of Americans' privacy. According to NSA spokeswoman Vanee Vines, if American communications are "incidentally collected during NSA's lawful signals intelligence activities," the agency follows "minimization procedures that are approved by the U.S. attorney general and designed to protect the privacy of United States persons."

As another U.S. official puts it, the NSA is "not wallowing willy-nilly" through Americans' idle online chatter. "We want high-grade ore."

To achieve that, the programs use complex algorithms that, in effect, operate like filters placed over a stream with holes designed to let certain pieces of information flow through. After the 2001 terrorist attacks, NSA widened the holes to capture more information when the government broadened its definition of what constitutes "reasonable" collection, according to a former top intelligence official.

The NSA's U.S. programs have been described in narrower terms in the documents released by former NSA contractor Edward Snowden. One, for instance, acquires Americans' phone records; another, called Prism, makes requests for stored data to Internet companies. By contrast, this set of programs shows the NSA has the capability to track almost anything that happens online, so long as it is covered by a broad court order.

The NSA programs are approved and overseen by the secret Foreign Intelligence Surveillance Court. NSA is required to destroy information on Americans that doesn't fall under exceptions to the rule, including information that is relevant to foreign intelligence, encrypted, or evidence of a crime.

The NSA is focused on collecting foreign intelligence, but the streams of data it monitors include both foreign and domestic communications. Inevitably, officials say, some U.S. Internet communications are scanned and intercepted, including both "metadata" about communications, such as the "to" and "from" lines in an email, and the contents of the communications

themselves.

Much, but not all, of the data is discarded, meaning some communications between Americans are stored in the NSA's databases, officials say. Some lawmakers and civil libertarians say that, given the volumes of data NSA is examining, privacy protections are insufficient.

Sen. Ron Wyden, an Oregon Democrat, in 2012 sought but failed to prohibit the agency from searching its databases for information on Americans without a warrant. He has also pushed intelligence agencies to detail how many Americans' communications have been collected and to explain whether purely domestic communications are retained in NSA's databanks. They have declined.

"Technology is moving us swiftly into a world where the only barriers to this kind of dragnet surveillance are the protections enshrined into law," Mr. Wyden says.

This month President Barack Obama proposed changes to NSA surveillance to improve oversight. Those proposed changes wouldn't alter the systems in the U.S. that NSA relies upon for some of its most sensitive surveillance.

The systems operate like this: The NSA asks telecom companies to send it various streams of Internet traffic it believes most likely to contain foreign intelligence. This is the first cut of the data.

These requests don't ask for all Internet traffic. Rather, they

focus on certain areas of interest, according to a person familiar with the legal process. "It's still a large amount of data, but not everything in the world," this person says.

The second cut is done by NSA. It briefly copies the traffic and decides which communications to keep based on what it calls "strong selectors"—say, an email address, or a large block of computer addresses that correspond to an organization it is interested in. In making these decisions, the NSA can look at content of communications as well as information about who is sending the data.

One U.S. official says the agency doesn't itself "access" all the traffic within the surveillance system. The agency defines access as "things we actually touch," this person says, pointing out that the telecom companies do the first stage of filtering.

The surveillance system is built on relationships with telecommunications carriers that together cover about 75% of U.S. Internet communications. They must hand over what the NSA asks for under orders from the secret Foreign Intelligence Surveillance Court. The firms search Internet traffic based on the NSA's criteria, current and former officials say.

Verizon Communications Inc., for example, has placed intercepts in the largest U.S. metropolitan areas, according to one person familiar with the technology. It isn't clear how much information these intercepts send to the NSA. A Verizon

spokesman declined to comment.

Not all telecommunications providers handle the government demands the same way, says the person familiar with the legal process. According to a U.S. official, lawyers at telecom companies serve as checks on what the NSA receives. "The providers are independently deciding what would be responsive," the official says.

Lawyers for at least one major provider have taken the view that they will provide access only to "clearly foreign" streams of data—for example, ones involving connections to ISPs in, say, Mexico, according to the person familiar with the legal process. The complexities of Internet routing mean it isn't always easy to isolate foreign traffic, but the goal is "to prevent traffic from Kansas City to San Francisco from ending up" with the NSA, the person says.

At times, the NSA has asked for access to data streams that are more likely to include domestic communications, this person says, and "it has caused friction." This person added that government officials have said some providers do indeed comply with requests like this.

The person says talks between the government and different telecoms about what constitutes foreign communications have "been going on for some years," and that some in the industry believe the law is unclear on Internet traffic. "Somebody should enunciate a rule," this person says.

Intelligence officials and the White House argue NSA's

surveillance provides early warnings of terror threats that don't respect geographic boundaries. "It's true we have significant capabilities," Mr. Obama said in his NSA remarks last week. "What's also true is we show a restraint that many governments around the world don't even think to do."

Mr. Obama and top intelligence officials say NSA's programs are overseen by all three branches of government, citing procedures approved by the secret surveillance court that require the NSA to eliminate "incidentally acquired" data on Americans. "If you say, 'We don't want the NSA to be scanning large amounts of traffic,' you're saying you don't want it to do its job," says one former official.

Blarney, Fairview, Oakstar, Lithium and Stormbrew were mentioned, but not fully explained, in documents released by Mr. Snowden. An NSA paper released this month mentioned several but didn't describe them beyond saying, "The government compels one or more providers to assist NSA with the collection of information responsive to the foreign intelligence need."

The system is built with gear made by Boeing Co.'s Narus subsidiary, which makes filtering technology, and Internet hardware manufacturers Cisco Systems Inc. and Juniper Networks Inc., among other companies, according to former intelligence officials and industry figures familiar with the equipment.

Narus didn't respond to requests for comment. Cisco and

Juniper declined to comment.

The NSA started setting up Internet intercepts well before 2001, former intelligence officials say. Run by NSA's secretive Special Services Office, these types of programs were at first designed to intercept communications overseas through arrangements with foreign Internet providers, the former officials say. NSA still has such arrangements in many countries, particularly in the Middle East and Europe, the former officials say.

Within NSA, former officials say, intelligence officers joked that the Blarney intercept program with AT&T was named in homage to the NSA program Shamrock, which intercepted telegraphic messages into and out of the U.S. and was an inspiration for the 1978 Foreign Intelligence Surveillance Act, which created the secret national-security court and placed intelligence activities under its supervision.

Blarney was in use before the 2001 terror attacks, operating at or near key fiber-optic landing points in the U.S. to capture foreign communications coming in and out of the country. One example is an AT&T facility in San Francisco that was revealed in 2006 during the debate over warrantless wiretapping. A similar facility was built at an AT&T site in New Jersey, former officials say.

After the 2001 attacks, a former official says, these intercept systems were expanded to include key Internet networks within the U.S. through partnerships with U.S. Internet

backbone providers. Amid fears of terrorist "sleeper cells" inside the U.S., the government under President George W. Bush also began redefining how much domestic data it could collect.

For the 2002 Winter Olympics in Salt Lake City, officials say, the Federal Bureau of Investigation and NSA arranged with Qwest Communications International Inc. to use intercept equipment for a period of less than six months around the time of the event. It monitored the content of all email and text communications in the Salt Lake City area.

At that point, the systems fed into the Bush administration's program of warrantless wiretapping, which circumvented the surveillance court on the authority of the president's power as commander in chief. The Bush administration came under criticism from lawmakers and civil libertarians for sidestepping court supervision.

The current legal backing for Blarney and its related programs stems from a section of a 2008 surveillance law. It permits the government, for foreign intelligence investigations, to snoop on foreigners "reasonably believed" to be outside the U.S.

Previously, the law had tighter standards. It allowed the government to spy on people if there were "probable cause" to believe they were an "agent of a foreign power."

NSA has discretion on setting its filters, and the system relies significantly on self-policing. This can result in improper collection that continues for years.

For example, a recent Snowden document showed that the surveillance court ruled that the NSA had set up an unconstitutional collection effort. Officials say it was an unintentional mistake made in 2008 when it set filters on programs like these that monitor Internet traffic; NSA uncovered the inappropriate filtering in 2011 and reported it.

"NSA's foreign intelligence collection activities are continually audited and overseen internally and externally," Ms. Vines says. "When we make a mistake in carrying out our foreign intelligence mission, we report the issue internally and to federal overseers and aggressively get to the bottom of it."

Another Snowden document describes the procedures NSA uses to protect American information that is retained. Any such information is "minimized," meaning that it is destroyed. The document highlights several exceptions, including encrypted communications and information of foreign intelligence significance.

Officials acknowledged some purely domestic communications are incidentally swept into the system. "We don't keep track of numbers of U.S. persons," a U.S. official says. "What we try to do is minimize any exposure."

When searching the data, intelligence officials say they are permitted to look only for information related to a "foreign intelligence interest." In practice, the NSA has latitude under that standard, and an American's communication could be read without a warrant, another U.S. official says.

Paul Kouroupas, a former executive at Global Crossing Ltd. and other telecom companies responsible for security and government affairs, says the checks and balances in the NSA programs depend on telecommunications companies and the government policing the system themselves. "There's technically and physically nothing preventing a much broader surveillance," he says.

An official at Global Crossing's parent, Level 3 Communications Inc., says the company complies with laws requiring it to assist government investigations and declined to disclose the assistance provided.

It is difficult to know how much domestic data NSA is inadvertently retaining. The filtering technology relies on algorithms to seek out valuable communications. A U.S. official says analysts guide the use of these algorithms to make them as precise as possible.

—Devlin Barrett contributed to this article.

Write to Siobhan Gorman at siobhan.gorman@wsj.com and Jennifer Valentino-DeVries at Jennifer.Valentino-DeVries@wsj.com