EXHIBIT 1

The New York Times

U.S.

N.S.A. Said to Search Content of Messages to and From U.S.

By CHARLIE SAVAGEAUG. 8, 2013

Stories from Our Advertisers

Continue reading the main story Share This Page
Continue reading the main story
Continue reading the main story

WASHINGTON â€" The National Security Agency is searching the contents of vast amounts of Americansâ€™ e-mail and text communications into and out of the country, hunting for people who mention information about foreigners under surveillance, according to intelligence officials.

The N.S.A. is not just intercepting the communications of Americans who are in direct contact with foreigners targeted overseas, a practice that government officials have openly acknowledged. It is also casting a far wider net for people who cite information linked to those foreigners, like a little used e-mail address, according to a senior intelligence official.

While it has long been known that the agency conducts extensive computer searches of data it vacuums up overseas, that it is systematically searching â€" without warrants â€" through the contents of Americansâ€™ communications that cross the border reveals more about the scale of its secret operations.

Continue reading the main story

Related in Opinion

Editorial: Breaking Through Limits on SpyingAUG. 8, 2013

It also adds another element to the unfolding debate, provoked by the disclosures of Edward J. Snowden, the former N.S.A. contractor, about whether the agency has infringed on Americansâ€™ privacy as it scoops up e-mails and phone data in its quest to ferret out foreign intelligence.

Government officials say the cross-border surveillance was authorized by a 2008 law, the FISA Amendments Act, in which Congress approved eavesdropping on domestic soil without warrants as long as the â€œtargetâ€ was a noncitizen abroad. Voice communications are not included in that surveillance, the senior official said.

Asked to comment, Judith A. Emmel, an N.S.A. spokeswoman, did not directly address surveillance of cross-border communications. But she said the agencyâ€™s activities were lawful and intended to gather intelligence not about Americans but about â€œforeign powers and their agents, foreign organizations, foreign persons or international terrorists.â€

â€œIn carrying out its signals intelligence mission, N.S.A. collects only what it is explicitly authorized to collect,â€ she said. â€œMoreover, the agencyâ€™s activities are deployed only in response to requirements for information to protect the country and its interests.â€

Hints of the surveillance appeared in a set of rules, leaked by Mr. Snowden, for how the N.S.A. may carry out the 2008 FISA law. One paragraph mentions that the agency â€œseeks to acquire communications about the target that are not to or from the target.â€ The pages were posted online by the newspaper The Guardian on June 20, but the telltale paragraph, the only rule marked â€œTop Secretâ€ amid 18 pages of restrictions, went largely overlooked amid other disclosures.

To conduct the surveillance, the N.S.A. is temporarily copying and then sifting through the contents of what is apparently most e-mails and other text-based communications that cross the border. The senior intelligence official, who, like other former and current government officials, spoke on condition of anonymity because of the sensitivity of the topic, said the N.S.A. makes a â€œclone of selected communication linksâ€ to gather the communications, but declined to specify details, like the volume of the data that passes through them.

Computer scientists said that it would be difficult to systematically search the contents of the communications without first gathering nearly all cross-border text-based data; fiber-optic networks work by breaking messages into tiny packets that flow at the speed of light over different pathways to their shared destination, so they would need to be captured and reassembled.

The official said that a computer searches the data for the identifying keywords or other â€œselectorsâ€ and stores those that match so that human analysts could later examine them. The remaining communications, the official said, are deleted; the entire process takes â€œa small number of seconds,â€ and the system has no ability to perform â€œretrospective searching.â€

The official said the keyword and other terms were â€œvery preciseâ€ to minimize the number of innocent American communications that were flagged by the program. At the same time, the official acknowledged that there had been times when changes by telecommunications providers or in the technology had led to inadvertent overcollection. The N.S.A. monitors for these problems, fixes them and reports such incidents to its overseers in the government, the official said.

The disclosure sheds additional light on statements intelligence officials have made recently, reassuring the public that they do not â€œtargetâ€ Americans for surveillance without warrants.

At a House Intelligence Committee oversight hearing in June, for example, a lawmaker pressed the deputy director of the N.S.A., John Inglis, to say whether the agency listened to the phone calls or read the e-mails and text messages of American citizens. Mr. Inglis replied, â€œWe do not target the content of U.S. person communications without a specific warrant anywhere on the earth.â€

Timothy Edgar, a former intelligence official in the Bush and Obama administrations, said that the rule concerning collection â€œaboutâ€ a person targeted for surveillance rather than directed at that person had provoked significant internal discussion.

â€œThere is an ambiguity in the law about what it means to â€˜targetâ€™ someone,â€ Mr. Edgar, now a visiting professor at Brown, said. â€œYou can never intentionally target someone inside the United States. Those are the words we were looking at. We were most concerned about making sure the procedures only target communications that have one party outside the United States.â€

The rule they ended up writing, which was secretly approved by the Foreign Intelligence Surveillance Court, says that the N.S.A. must ensure that one of the participants in any conversation that is acquired when it is searching for conversations about a targeted foreigner must be outside the United States, so that the surveillance is technically directed at the foreign end.

Americansâ€™ communications singled out for further analysis are handled in accordance with â€œminimizationâ€ rules to protect privacy approved by the surveillance court. If private information is not relevant to understanding foreign intelligence, it is deleted; if it is relevant, the agency can retain it and disseminate it to other agencies, the rules show.

While the paragraph hinting at the surveillance has attracted little attention, the American Civil Liberties Union did take note of the â€œabout the targetâ€ language in a June 21 post analyzing the larger set of rules, arguing that the language could be interpreted as allowing â€œbulkâ€ collection of international communications, including of those of Americans.

Jameel Jaffer, a senior lawyer at the A.C.L.U., said Wednesday that such â€œdragnet surveillance will be poisonous to the freedoms of inquiry and associationâ€ because people who know that their communications will be searched will change their behavior.

â€œTheyâ€™ll hesitate before visiting controversial Web sites, discussing controversial topics or investigating politically sensitive questions,â€ Mr. Jaffer said. â€œIndividually, these hesitations might appear to be inconsequential, but the accumulation of them over time will change citizensâ€™ relationship to one another and to the government.â€

The senior intelligence official argued, however, that it would be inaccurate to portray the N.S.A. as engaging in â€œbulk collectionâ€ of the contents of communications. â€œÂ â€˜Bulk collectionâ€™ is when we collect and retain for some period of time that lets us do retrospective analysis,â€ the official said. â€œIn this case, we do not do that, so we do not consider this â€˜bulk collection.â€™Â â€

Stewart Baker, a former general counsel for the N.S.A., said that such surveillance could be valuable in identifying previously unknown terrorists or spies inside the United States who unwittingly reveal themselves to the agency by discussing a foreign-intelligence â€œindicator.â€ He cited a situation in which officials learn that Al Qaeda was planning to use a particular phone number on the day of an attack.

â€œIf someone is sending that number out, chances are they are on the inside of the plot, and I want to find the people who are on the inside of the plot,â€ he said.

The senior intelligence official said that the â€œabout the targetâ€ surveillance had been valuable, but said it was difficult to point to any particular terrorist plot that would have been carried out if the surveillance had not taken place. He said it was one tool among many used to assemble a â€œmosaicâ€ of information in such investigations. The surveillance was used for other types of foreign-intelligence collection, not just terrorism investigations, the official said.

There has been no public disclosure of any ruling by the Foreign Intelligence Surveillance Court explaining its legal analysis of the 2008 FISA law and the Fourth Amendment as allowing â€œabout the targetâ€ searches of Americansâ€™ cross-border communications. But in 2009, the Justice Departmentâ€™s Office of Legal Counsel signed off on a similar process for searching federal employeesâ€™ communications without a warrant to make sure none contain malicious computer code.

That opinion, by Steven G. Bradbury, who led the office in the Bush administration, may echo the still-secret legal analysis. He wrote that because that system, called EINSTEIN 2.0, scanned communications traffic â€œonly for particular malicious computer codeâ€ and there was no authorization to acquire the content for unrelated purposes, it â€œimposes, at worst, a minimal burden upon legitimate privacy rights.â€

A version of this article appears in print on August 8, 2013, on page A1 of the New York edition with the headline: Broader Sifting Of Message Data By N.S.A. Is Seen. Order Reprints| Today's Paper|Subscribe

- Letters
- Sunday Review
- Taking Note
- Room for Debate
- Public Editor
- Video: Opinion

Arts

- Today's Arts
- Art & Design
- ArtsBeat
- Books
- Dance
- Movies
- Music
- N.Y.C. Events Guide
- Television
- Theater
- Video Games
- Video: Arts

Living

- Automobiles
- Crossword
- Food
- Education
- Fashion & Style
- Health
- Jobs
- Magazine
- N.Y.C. Events Guide
- Real Estate
- T Magazine
- Travel
- Weddings & Celebrations

Listings & More

- Classifieds
- Tools & Services
- Times Topics
- Public Editor
- N.Y.C. Events Guide
- TV Listings
- Blogs
- Cartoons
- Multimedia
- Photography