THE DISPATCH

How the NSA Ends Up With Information on Americans Without Targeting Them

Tripp Grebe

July 16, 2021

During a June 28 show, Fox News's Tucker Carlson told his viewers that a whistleblower within the U.S. government had warned him that the National Security Agency (NSA) was monitoring his electronic communications and was planning to leak them in an attempt to take his show off the air. This week, a group of House Republicans led by Rep. Louie Gohmert sent a letter to the NSA demanding more information.

Carlson's accusation prompted the NSA to make a rare public statement denying that Carlson had been personally targeted—but the statement didn't deny that any of Carlson's communications had been collected by the agency.

Axios later reported that Carlson was communicating with Kremlin intermediaries in the United States about setting up an interview with Vladimir Putin, which potentially could have created a scenario in which the NSA incidentally collected Carlson's communications.

The NSA's mission is to support national security and foreign policy by protecting classified national security information and collecting information about foreign adversaries' secret communications. It typically carries out its mission through three separate operations: hacking operations, overseas collection, and domestic collection.

The Office of Tailored Access Operations is the cyber-warfare intelligence gathering unit of the NSA that runs its hacking operations. Consisting of more than 1,000 hackers, analysts, and engineers, the TAO infiltrates and gathers data from computer systems of foreign entities.

The TAO has been confirmed to have targeted the systems of the Chinese government, OPEC, and Mexico's Secretariat of Public Security—and has reportedly enjoyed reasonable success, thanks to cooperation from American telecom companies.

The NSA uses various tools and programs to collect data from foreign citizens, leaders, and organizations to carry out its overseas collection operation.

Data is collected from unsecured communications like radio broadcasts, the internet, and telephone calls, and secure communications such as military, diplomatic, or secret government communications. The NSA then uses this information to build a database that helps the agency determine potential national security threats.

To obtain approval to conduct targeted surveillance of foreign entities located outside the United States, the NSA must abide by the Section 702 provision in the FISA Amendment Act of 2008.

Under Section 702, the attorney general and director of national intelligence must submit targeted areas of foreign intelligence to the Foreign Intelligence Surveillance Court (FISC) that the NSA can use Section 702 to collect. They must also submit rules designed to protect any U.S. person's information incidentally acquired during foreign surveillance, known as minimization procedures.

The FISC reviews the certifications and procedures to ensure they comply with both FISA protocols and the Fourth Amendment, then issues a written opinion. If the FISC approves the targeted areas of foreign intelligence and the minimization procedures, the attorney general and DNI can order the intelligence community to begin surveillance.

While the NSA operates under a cloud of secrecy, it appears to have a fairly robust overseas collection operation—as they have intercepted the communications of European Union leaders, the United Nations, and German Chancellor Angela Merkel.

Since the NSA is a foreign-directed agency, it is supposed to restrict its surveillance programs to foreign entities, but sometimes, the agency ends up with collection the information of U.S. citizens. There are two ways in which the NSA can end up collecting such information: incidental collection or targeted collection.

Julian Sanchez, a senior fellow at the Cato Institute, explains how the NSA could incidentally collect U.S. citizens' information.

"Incidental collection is when the NSA is targeting a foreign person, usually outside of the United States, and that person is in contact with a U.S. citizen. And in the process of surveilling the foreign person, the U.S. person's communications get swept up," Sanchez told *The Dispatch.* "If you call or email someone overseas who happens to be on a list of intelligence targets, your communication could get swept up."

Targeted collection of U.S. citizens' communications is not a directive of the NSA. To obtain a surveillance warrant against a person inside of the United States, the Department of Justice must present evidence to the FISC that justifies the warrant. If the court approves the warrant, then intelligence agencies may begin surveilling communications of individual in question.

"The NSA itself is not supposed to target any person inside of the United States, but on occasion, the FBI or DOJ may target a person inside of the United States and ask for the NSA's help in executing that surveillance," Sanchez explained to *The Dispatch.*

Even if a person's communications are incidentally collected, the NSA likely knows his or her identity when it initially collects communication data. It isn't difficult to figure out if the agency has collected an email address or phone number.

However, after the NSA has collected the foreign intelligence that an individual's communication was swept up in, unless knowing his or her name is essential to understand the intelligence, the agency will mask the person's name and describe him or her in a way that doesn't reveal the individual's identity when the intelligence is shared with other agencies.

Once other agencies like the FBI or CIA receive the intelligence, they can request the name to be unmasked if they believe knowing it is essential to understanding the intelligence.

Unmasking is a fairly common occurrence; last year the NSA distributed 2,648 reports containing "masked" U.S. person identities and 1,351 reports in which at least one U.S. person's identity was included. In 2020, after a specific request from another agency, the NSA unmasked the identities of 9,354 U.S. persons.

It's not unthinkable that an intelligence agency might collect a journalist's communications—the Obama administration famously seized two months of telephone records of reporters and editors at the Associated Press, citing investigations into leaks of sensitive national security information, and the Trump Justice Department obtained three *Washington Post* journalists' phone records.

Because the NSA itself does not target Americans, Carlson's claim that the NSA was "spying" on him would mean that the Biden Justice Department presented enough evidence to the FISA court that showed Carlson to be a national security threat, thereby justifying a surveillance warrant.

A much more likely scenario is that the intermediaries Carlson was in communication with were under foreign surveillance and Carlson's communications were swept up through incidental collection as a result.