

The New York Times

Obama Administration Set to Expand Sharing of Data That N.S.A. Intercepts

By CHARLIE SAVAGE FEB. 25, 2016



President Obama, meeting Thursday with his National Security Council, wants more intelligence experts to see information intercepted by the National Security Agency. Credit Zach Gibson/The New York Times

WASHINGTON — The Obama administration is on the verge of permitting the National Security Agency to share more of the private communications it intercepts with other American intelligence agencies without first applying any privacy protections to them, according to officials familiar with the deliberations.

The change would relax longstanding restrictions on access to the contents of the phone calls and email the security agency vacuums up around the world, including bulk collection of satellite transmissions, communications between foreigners as they cross network switches in the United States, and messages acquired overseas or provided by allies.

The idea is to let more experts across American intelligence gain direct access to unprocessed information, increasing the chances that they will recognize any possible nuggets of value. That also means more officials will be looking at private messages —

not only foreigners' phone calls and emails that have not yet had irrelevant personal information screened out, but also communications to, from, or about Americans that the N.S.A.'s foreign intelligence programs swept in incidentally.

Civil liberties advocates criticized the change, arguing that it will weaken privacy protections. They said the government should disclose how much American content the N.S.A. collects incidentally — which agency officials have said is hard to measure — and let the public debate what the rules should be for handling that information.

“Before we allow them to spread that information further in the government, we need to have a serious conversation about how to protect Americans' information,” said Alexander Abdo, an American Civil Liberties Union lawyer.

Robert S. Litt, the general counsel in the office of the Director of National Intelligence, said that the administration had developed and was fine-tuning what is now a 21-page draft set of procedures to permit the sharing.

The goal for the final rules, Brian P. Hale, a spokesman for the office, said in a statement, is “to ensure that they protect privacy, civil liberties and constitutional rights while enabling the sharing of information that is important to protect national security.”

Until now, National Security Agency analysts have filtered the surveillance information for the rest of the government. They search and evaluate the information and pass only the portions of phone calls or email that they decide is pertinent on to colleagues at the Central Intelligence Agency, the Federal Bureau of Investigation and other agencies. And before doing so, the N.S.A. takes steps to mask the names and any irrelevant information about innocent Americans.

The new system would permit analysts at other intelligence agencies to obtain direct access to raw information from the N.S.A.'s surveillance to evaluate for themselves. If they pull out phone calls or email to use for their own agency's work, they would apply the privacy protections masking innocent Americans' information — a process known as “minimization” — at that stage, Mr. Litt said.

Executive branch officials have been developing the new framework and system for years. President George W. Bush set the change in motion through a little-noticed line in a 2008 executive order, and the Obama administration has been quietly developing a framework for how to carry it out since taking office in 2009.

The executive branch can change its own rules without going to Congress or a judge for permission because the data comes from surveillance methods that lawmakers did not include in the main law that governs national security wiretapping, the Foreign Intelligence Surveillance Act, or FISA.

FISA covers a narrow band of surveillance: the collection of domestic or international communications from a wire on American soil, leaving most of what the N.S.A. does uncovered. In the absence of statutory regulation, the agency's other surveillance programs are governed by rules the White House sets under a Reagan-era directive called [Executive Order 12333](#).

Mr. Litt declined to make available a copy of the current draft of the proposed procedures.

“Once these procedures are final and approved, they will be made public to the extent consistent with national security,” Mr. Hale said. “It would be premature to draw conclusions about what the procedures will provide or authorize until they are finalized.”

Among the things they would not address is what the draft rules say about searching the raw data using names or keywords intended to bring up Americans’ phone calls or email that the security agency gathered “incidentally” under the 12333 surveillance programs — including whether F.B.I. agents may do so when working on ordinary criminal investigations.

Under current rules for data gathered under a parallel program — the no-warrant surveillance program governed by the FISA Amendments Act — N.S.A. and C.I.A. officials may search for Americans’ information only if their purpose is to find foreign intelligence, but F.B.I. agents may conduct such a search for intelligence or law enforcement purposes. Some lawmakers have proposed requiring the government to obtain a warrant before conducting such a search.

In 2013, The Washington Post [reported](#), based on documents leaked by the former intelligence contractor Edward J. Snowden, that the N.S.A. and its British counterpart, Government Communications Headquarters, had tapped into links connecting Google’s and Yahoo’s data centers overseas and that the American spy agency had collected millions of records a day from them. The companies have [since taken steps to encrypt](#) those links.

That collection occurred under 12333 rules, which had long prohibited the N.S.A. from sharing raw information gathered from the surveillance it governed with other members of the intelligence community before minimization. The same rule had also long applied to sharing information gathered with FISA wiretaps.

But after the attacks of Sept. 11, 2001, the Bush administration began an effort to tear down barriers that impeded different parts of the government from working closely and sharing information, especially about terrorism.

In 2002, for example, it won permission, then secret, from the intelligence court permitting the C.I.A., the F.B.I. and the N.S.A. to share raw FISA wiretap information. The government did not disclose that change, which was first reported in a 2014 [New York Times article](#) based on documents disclosed by Mr. Snowden.

In August 2008, Mr. Bush changed 12333 to permit the N.S.A. to share unevaluated surveillance information with other intelligence agencies once procedures were developed.

Intelligence officials began working in 2009 on how the technical system and rules would work, Mr. Litt said, eventually consulting the Defense and Justice Departments. This month, the administration briefed the Privacy and Civil Liberties Oversight Board, an independent five-member watchdog panel, seeking input. Before they go into effect, they must be approved by James R. Clapper, the intelligence

director; Loretta E. Lynch, the attorney general; and Ashton B. Carter, the defense secretary.

“We would like it to be completed sooner rather than later,” Mr. Litt said. “Our expectation is months rather than weeks or years.”

http://www.nytimes.com/2016/02/26/us/politics/obama-administration-set-to-expand-sharing-of-data-that-nsa-intercepts.html?rref=collection%2Ftimestopic%2FNational%20Security%20Agency&action=click&contentCollection=timestopics®ion=stream&module=stream_unit&version=latest&contentPlacement=8&pgtype=collection