Chicago Tribune

NSA breaks privacy rules, audit says

Documents show some significant violations of law

By: Barton Gellman – August 15, 2013

The National Security Agency has broken privacy rules or overstepped its legal authority thousands of times each year since Congress granted the agency broad new powers in 2008, according to an internal audit and other top-secret documents.

Most of the infractions involve unauthorized surveillance of Americans or foreign intelligence targets in the United States, both of which are restricted by law and executive order. They range from significant violations of law to typographical errors that resulted in unintended interception of U.S. e-mails and telephone calls.

The documents, provided earlier this summer to The Washington Post by former NSA contractor Edward Snowden, include a level of detail and analysis that is not routinely shared with Congress or the special court that oversees surveillance. In one of the documents, agency personnel are instructed to remove details and substitute more generic language in reports to the Justice Department and the Office of the Director of National Intelligence.

In one instance, the NSA decided that it need not report the unintended surveillance of Americans. A notable example in 2008 was the interception of a "large number" of calls placed from Washington when a programming error confused U.S. area code 202 for 20, the international dialing code for Egypt, according to a "quality assurance" review that was not distributed to the NSA's oversight staff.

In another case, the Foreign Intelligence Surveillance Court, which has authority over some NSA operations, did not learn about a new collection method until it had been in operation for many months. The court ruled it unconstitutional.

The Obama administration has provided almost no public information about the NSA's compliance record. In June, after promising to explain the NSA's record in "as transparent a way as we possibly can," Deputy Attorney General James Cole described extensive safeguards and oversight that keep the agency in check. "Every now and then, there may be a mistake," Cole said in congressional testimony.

The NSA audit obtained by The Post, dated May 2012, counted 2,776 incidents in the preceding 12 months of unauthorized collection, storage, access to or distribution of legally protected communications. Most were unintended. Many involved failures of due diligence or violations of standard operating procedure. The most serious incidents included a violation of a court order and unauthorized use of data about more than 3,000 Americans and green-card holders.

In a statement in response to questions for this article, the NSA said it attempts to identify problems "at the earliest possible moment, implement mitigation measures wherever possible, and drive the numbers down." The government was made aware of The Post's intention to publish the documents that accompany this article online.

"We're a human-run agency operating in a complex environment with a number of different regulatory regimes, so at times we find ourselves on the wrong side of the line," a senior NSA official said in an interview, speaking with White House permission on the condition of anonymity.

"You can look at it as a percentage of our total activity that occurs each day," he said. "You look at a number in absolute terms that looks big, and when you look at it in relative terms, it looks a little different."

There is no reliable way to calculate from the number of recorded compliance issues how many Americans have had their communications improperly collected, stored or distributed by the NSA.

The causes and severity of NSA infractions vary widely. One in 10 incidents is attributed to a typographical error in which an analyst enters an incorrect query and retrieves data about U.S phone calls or e-mails.

But the more serious lapses include unauthorized access to intercepted communications, the distribution of protected content and the use of automated systems without built-in safeguards to prevent unlawful surveillance.

The May 2012 audit, intended for the agency's top leaders, counts only incidents at NSA's Fort Meade, Md. headquarters and other facilities in the Washington area. Three government officials, speaking on the condition of anonymity to discuss classified matters, said the number would be substantially higher if it included other NSA operating units and regional collection centers.

Senate Intelligence Committee Chairman Dianne Feinstein, D-Calif., who did not receive a copy of the 2012 audit until The Post asked her staff about it, said in a statement late Thursday that the committee "can and should do more to independently verify that NSA's operations are appropriate, and its reports of compliance incidents are accurate."

Despite the quadrupling of NSA's oversight staff after a series of significant violations in 2009, the rate of infractions increased throughout 2011 and early 2012. An NSA spokesman declined to disclose whether the trend has continued since last year.

One major problem is largely unpreventable, the audit says, because current operations rely on technology that cannot quickly determine whether a foreign mobile phone has entered the United States.

In what appears to be one of the most serious violations, the NSA diverted large volumes of international data passing through fiber-optic cables in the United States into a repository where the material could be stored temporarily for processing and selection.

The operation to obtain what the agency called "multiple communications transactions" collected and commingled U.S. and foreign e-mails, according to an article in SSO News, a top-secret internal newsletter of the NSA's Special Source Operations unit. NSA lawyers told the court that the agency could not practicably filter out the communications of Americans.

In October 2011, months after the program got underway, the Foreign Intelligence Surveillance Court ruled that the collection effort was unconstitutional. The court said that the methods used were "deficient on statutory and constitutional grounds," according to a top-secret summary of the opinion, and it ordered the NSA to comply with standard privacy protections or stop the program.

James R. Clapper Jr., the director of national intelligence, has acknowledged that the court found the NSA in breach of the Fourth Amendment, which prohibits unreasonable searches and seizures, but the Obama administration has fought a Freedom of Information lawsuit that seeks the opinion.

Generally, the NSA reveals nothing in public about its errors and infractions. The unclassified versions of the administration's semi-annual reports to Congress feature blacked-out pages under the headline, "Statistical Data Relating to Compliance Incidents."

Members of Congress may read the unredacted documents, but only in a special secure room and are not allowed to take notes. Fewer than 10 percent of lawmakers employ a staff member who has the security clearance to read the reports and provide advice about their meaning and significance.

The limited portions of the reports that can be read by the public acknowledge "a small number of compliance incidents."

Under NSA auditing guidelines, the incident count does not usually disclose the number of Americans affected.

"What you really want to know, I would think, is how many innocent U.S. person communications are, one, collected at all, and two, subject to scrutiny," said Julian Sanchez, a research scholar and close student of the NSA at the Cato Institute.

The documents provided by Snowden offer only glimpses of those questions. Some reports make clear that an unauthorized search produced no records. But a single "incident" in February 2012 involved the unlawful retention of 3,032 files that the surveillance court had ordered the NSA to destroy, according to the May 2012 audit. Each file contained an undisclosed number of telephone call records.

One of the documents sheds new light on a statement by NSA Director Keith Alexander last year that "we don't hold data on U.S. citizens."

Some Obama administration officials, speaking on the condition of anonymity, have defended Alexander with assertions that the agency's internal definition of "data" does not cover "metadata" such as the trillions of American call records that the NSA is now known to have collected and stored since 2006. Those records include the telephone numbers of the parties and the times and durations of conversations, among other details, but not their content or the names of callers.

The NSA's authoritative definition of data includes those call records. "Signals Intelligence Management Directive 421," which is quoted in secret oversight and auditing guidelines, states that "raw SIGINT data . . . includes, but is not limited to, unevaluated and/or unminimized transcripts, gists, facsimiles, telex, voice, and some forms of computer-generated data, such as

call event records and other Digital Network Intelligence (DNI) metadata as well as DNI message text."

In the case of the collection effort that confused calls placed from Washington with those placed from Egypt, it is unclear what the NSA meant by a "large number" of intercepted calls. A spokesman declined to discuss the matter.

The NSA has different reporting requirements for each branch of government and each of its legal authorities. The "202" collection was deemed irrelevant to any of them. "The issue pertained to Metadata ONLY so there were no defects to report," according to the author of the secret memo from March 2013.

The large number of database query incidents, which involve previously collected communications, confirms long-standing suspicions that the NSA's vast data banks â" with code names such as MARINA, PINWALE and XKEYSCORE â" house a considerable volume of information about Americans. Ordinarily the identities of people in the United States are masked, but intelligence "customers" may request unmasking, either one case at a time or in standing orders.

In dozens of cases, NSA personnel made careless use of the agency's extraordinary powers, according to individual auditing reports. One team of analysts in Hawaii, for example, asked a system called DISHFIRE to find any communications that mentioned both the Swedish manufacturer Ericsson and "radio" or "radar" â" a query that could just as easily have collected on people in the United States as on their Pakistani military target.

The NSA uses the term "incidental" when it sweeps up the records of an American while targeting a foreigner or a U.S. person who is believed to be involved in terrorism. Official guidelines for NSA personnel say that kind of incident, pervasive under current practices, "does not constitute a . . . violation" and "does not have to be reported" to the NSA inspector general for inclusion in quarterly reports to Congress. Once added to its databases, absent other restrictions, the communications of Americans may be searched freely.

In one required tutorial, NSA collectors and analysts are taught to fill out oversight forms without giving "extraneous information" to "our FAA overseers." FAA is a reference to the FISA Amendments Act of 2008, which granted broad new authorities to the NSA in exchange for regular audits from the Justice Department and the office of the Director of National Intelligence and periodic reports to Congress and the surveillance court.

Using real-world examples, the "Target Analyst Rationale Instructions" explain how NSA employees should strip out details and substitute generic descriptions of the evidence and analysis behind their targeting choices.

"I realize you can read those words a certain way," said the high-ranking NSA official who spoke with White House authority, but the instructions were not intended to withhold information from auditors. "Think of a book of individual recipes," he said. Each target "has a short, concise description," but that is "not a substitute for the full recipe that follows, which our overseers also have access to."