The Washington Post

SUNDAY, JUNE 30, 2013

Judge defends role in spying

NO 'COORDINATION' WITH EXECUTIVE

Special court held NSA to account, jurist says

BY CAROL D. LEONNIG, ELLEN NAKASHIMA AND BARTON GELLMAN

Recent leaks of classified documents have pointed to the role of a special court in enabling the government's secret surveillance programs, but members of the court are chafing at the suggestion that they were collaborating with the executive branch.

A classified 2009 draft report by the National Security Agency's inspector general relayed some details about the interaction between the court's judges and the NSA, which sought approval for the Bush administration's top-secret domestic surveillance programs. The report was described in The Washington Post on June 16 and released in full Thursday by The Post and the British newspaper the Guardian.

U.S. District Judge Colleen Kollar-Kotelly, the former chief judge of the Foreign Intelligence Surveillance Court, took the highly unusual step Friday of voicing open frustration at the account in the report and the court's inability to explain its decisions.

"In my view, that draft report contains major omissions, and some inaccuracies, regarding the actions I took as Presiding Judge of the FISC and my interactions with Executive Branch officials," Kollar-Kotelly said in a statement to The Post. It was her first public comment describing her work on the intelligence court.

The inspector general's draft report is among the many documents leaked by former NSA contractor Edward Snowden, touching off a roiling national debate about the proper balance between the government's reach into Americans' lives and the effort to protect the nation in the Internet age.

The document portrays the surveillance court as "amenable" to the government's legal theory to "re-create" authority for the Internet metadata program that had initially been authorized by President George W. Bush without court or congressional approval. The program was shut down in March 2004 when acting Attorney General James B. Comey and senior leaders at the Justice Department threatened to resign over what they felt was an illegal program.

Kollar-Kotelly disputed the NSA report's suggestion of a fairly high level of coordination between the court and the NSA and Justice in 2004 to re-create certain authorities under the Foreign Intelligence Surveillance Act, the 1978 law that created the court in response to abuses of domestic surveillance in the 1960s and 1970s.

"That is incorrect," she said. "I participated in a process of adjudication, not 'coordination' with the executive branch. The discussions I had with executive branch officials were in most respects typical of how I and other district court judges entertain applications for criminal wiretaps under Title III, where issues are discussed ex parte."

The perception that the court works too closely with the government arises in large part from the tribunal's "ex parte" nature, which means that unlike in a traditional court, there is no legal sparring between adversaries with the judge as arbiter. Instead, a Justice Department official makes

the case for the government agency seeking permission to carry out surveillance inside the United States. No one speaks for the target of the surveillance or the company that is ordered to allow its networks to be tapped or to turn over its customers' data.

Some critics say the court is a rubber stamp for government investigators because it almost never has turned down a warrant application. However, that high approval rate doesn't take into account changes the court requires in some requests and other applications that the government withdraws.

For about 30 years, the court was on the sixth floor of the Justice Department's headquarters, down the hall from the officials who would argue in front of it. (The court moved to the District's federal courthouse in 2009.) "There is a collaborative process that would be unnatural in the public, criminal court setting," said a former Justice official familiar with the court ,who spoke on the condition of anonymity because of the subject's sensitivity.

Kollar-Kotelly, who was the court's chief judge from 2002 to 2006, said she could not comment further on the matter because "the underlying subjects" in the report generally remain classified by the executive branch.

Other judges on the court have confided to colleagues their frustration at the court's portrayal, according to people familiar with their discussion.

The inspector general's report, combined with persistent refusals by the government to declassify the opinions, have left the public in the dark about the court's legal justifications for approving the broad surveillance programs.

"The court is a neutral party, not a collaborator or arm of the government," said one government official close to the court. "But the information out there now leaves people wondering how and why the court endorsed these programs."

The court historically has authorized in secret hearings classified warrants to wiretap the calls and monitor the movements of suspected criminals. After the terrorist attacks of Sept. 11, 2001, far-reaching programs to gather Internet and telephone content and metadata were launched under presidential authority, without congressional action or approval from the surveillance court.

The Internet metadata portion of that program had to be revamped after Comey and other Justice officials threatened to resign. Metadata are information indicating facts such as an e-mail's sender and recipient and its time and date, but not its content.

In May 2004, the NSA briefed Kollar-Kotelly on the technical aspects of that program's collection, according to the report. She also met with the NSA director, Lt. Gen. Michael V. Hayden, on two successive Saturdays during the summer of 2004 to discuss the issue, the report said.

"It was very professional," Hayden said in an interview. "We of course had to explain to her what it was we had been doing, what it was we wanted to do, how we would do it, what kind of safeguards we felt able to put in. We left it to her judgment whether there was proportionality in terms of was this worth doing, in the balance between security and liberty."

He said in response to her concerns, the agency made some technical adjustments so that "the odds were greater that you'd pick up fewer protected communications of U.S. persons."

Said Hayden: "She wasn't in league with us. We were down there presenting what we thought was appropriate."

On July 14, 2004, the surveillance court for the first time approved the gathering of information by the NSA, which created the equivalent of a digital vault to hold Internet metadata. Kollar-Kotelly's order authorized the metadata program under a FISA provision known as the "pen register/trap and trace," or PRTT.

The ruling was a secret not just to the public and most of Congress, but to all of Kollar-Kotelly's surveillance court colleagues. Under orders from the president, none of the court's other 10 members could be told about the Internet metadata

program, which was one prong of a larger and highly classified data-gathering effort known as the President's Surveillance Program, or PSP.

But the importance of her order — which approved the collection based on a 1986 law typically used for phone records — was hard to overstate.

"The order essentially gave NSA the same authority to collect bulk Internet metadata that it had under the PSP," the inspector general's report said, with some minor caveats including reducing the number of people who could access the records.

On May 24, 2006, Kollar-Kotelly signed another order, this one authorizing the bulk collection of phone metadata from U.S. phone companies, under a FISA provision known as Section 215, or the "business records provision," of the USA Patriot Act.

As with the PRTT order, the Justice Department and NSA "collaboratively designed the application, prepared declarations and responded to questions from court advisers," the inspector general's report said. "Their previous experience in drafting the PRTT order made this process more efficient."

The court also agreed in 2007 to permit the government to collect the content of e-mails and phone calls to and from the United States when "there is probable cause to believe" that one of the parties is a member of al-Qaeda or an associated terrorist group. That program, known today as PRISM and described in documents obtained by The Washington Post, eventually was authorized by Congress.

Kollar-Kotelly could be a stern taskmaster when she thought the NSA was overstepping its bounds. In 2004, she temporarily shut down the government's surveillance program when she learned of a key NSA failure, The Post reported in 2006. The agency was not properly walling off information gained in warrantless surveillance and may have been using the information to obtain court warrants, which was forbidden. In 2005, the problem resurfaced and she issued a strong warning to the government that it had to fix the problem or would face trouble obtaining court warrants.

Kollar-Kotelly "understood the problems that the government, particularly the Defense Department and the intelligence community, were facing in trying to keep this country safe," said Robert L. Deitz, former NSA general counsel under Hayden.

But, he said, the court was no rubber stamp. "The judges ask searching questions," he said. "If they don't get the right answer, they don't stamp things 'reject.' They say, 'I'm not signing this.' Then we go back and say, 'Okay, we've got to do this the following way.'"

Still secret are the 2004 decision accompanying the PRTT court order and the legal opinion accompanying the 2006 business records order.

A former senior Justice Department official said he believes the government should consider releasing declassified summaries of relevant opinions.

"I think it would help" quell the "furor" raised by the recent disclosures, he said. "In this current environment, you may have to lean forward a little more in declassifying stuff than you otherwise would. You might be able to prepare reasonable summaries that would be helpful to the American people."

Lawmakers and civil-liberties advocates have been pushing the Obama administration for several years to declassify these opinions and other opinions from Justice's Office of Legal Counsel that explain the legal justification for these programs.

The Office of the Director of National Intelligence has led an effort to review these opinions to see what, if anything, can be declassified. But Robert S. Litt, ODNI general counsel, has argued that declassification can be difficult when so much of the legal reasoning is intertwined with facts that need to remain secret lest they tip off enemies about surveillance methods.

Still, the former official explained, segregating relevant facts from classified material is routinely done in criminal proceedings under the Classified Information Procedures Act. In those cases, the govern-

ment can extract the information that is relevant to the defense, the judge approves it, and it is provided to the defense.

"This is not unheard-of in the unclassified world, and some kind of summary document can be generated," the former official said. "Maybe that's a middle ground that can be done."

carol.leonnig@washpost.com
ellen.nakashima@washpost.com
barton.gellman@washpost.com

Sari Horwitz contributed to this report.

Inner workings of a secret surveillance program

BY BARTON GELLMAN AND TODD LINDEMAN

The National Security Agency's PRISM progam, which collects intelligence from Microsoft, Google, Yahoo, Apple and other tech giants, is "targeted" at foreigners. But it also collects the e-mail, voice, text and video chats of an unknown number of Americans — "inadvertently," "incidentally" or deliberately if an American is conversing with a foreign target overseas. Here are new details on how the program works, from Top Secret documents and interviews.

HOW THE PRISM PROGRAM WORKS

Targeting a "selector"

An NSA analyst types one or more search terms, or "selectors." Selectors may refer to people (by name, e-mail address, phone number or some other digital signature), organizations or subjects such as the sale of specialized parts for uranium enrichment.

Along with the selectors, the analyst must fill out an electronic form that specifies the foreign-intelligence purpose of the search and the basis for the analyst's "reasonable belief" that the search will not return results for U.S. citizens, permanent residents or anyone else who is located in the United States.

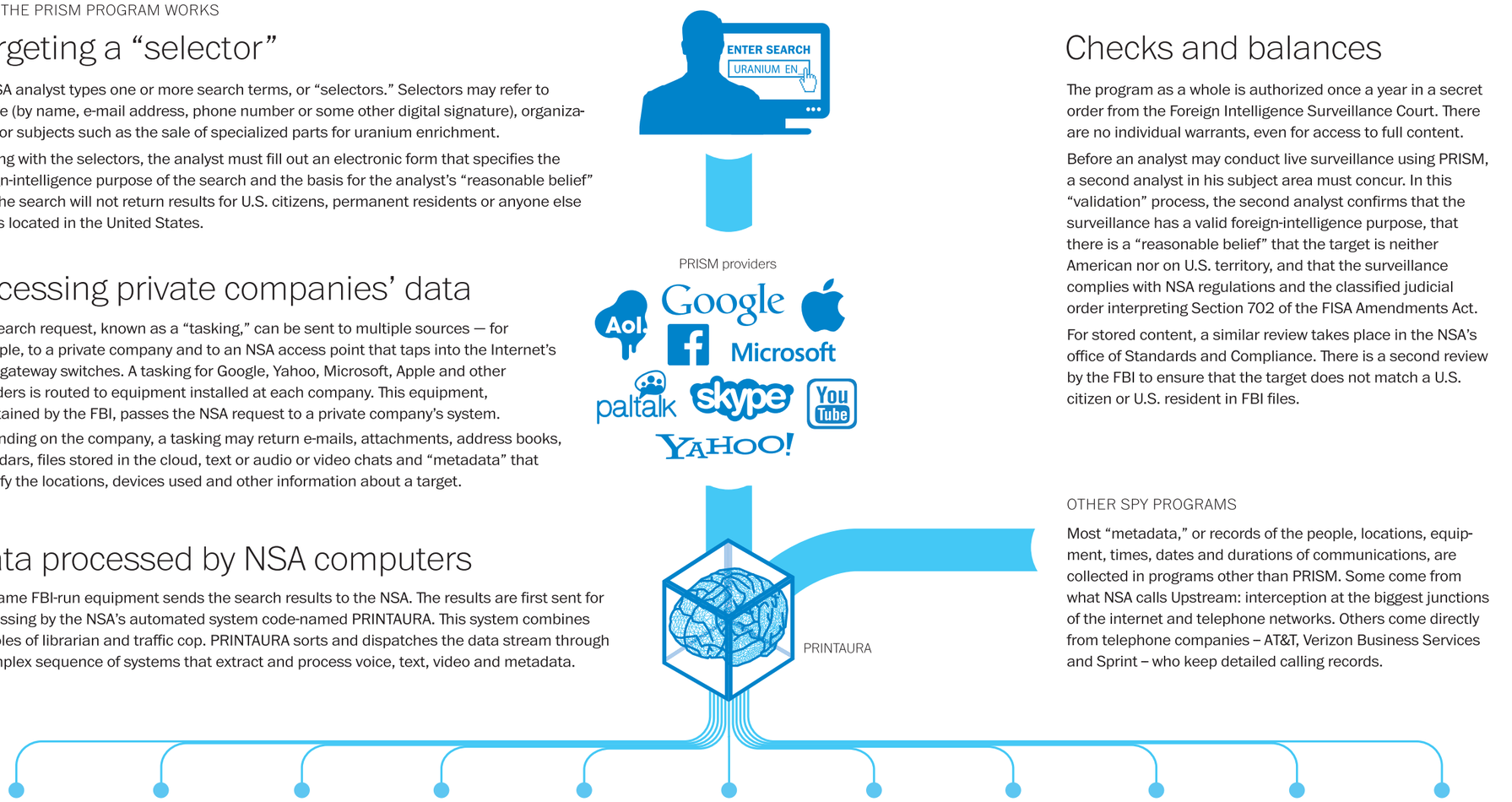
Accessing private companies' data

The search request, known as a "tasking," can be sent to multiple sources — for example, to a private company and to an NSA access point that taps into the Internet's main gateway switches. A tasking for Google, Yahoo, Microsoft, Apple and other providers is routed to equipment installed at each company. This equipment, maintained by the FBI, passes the NSA request to a private company's system.

Depending on the company, a tasking may return e-mails, attachments, address books, calendars, files stored in the cloud, text or audio or video chats and "metadata" that identify the locations, devices used and other information about a target.

Data processed by NSA computers

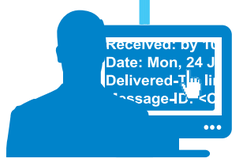
The same FBI-run equipment sends the search results to the NSA. The results are first sent for processing by the NSA's automated system code-named PRINTAURA. This system combines the roles of librarian and traffic cop. PRINTAURA sorts and dispatches the data stream through a complex sequence of systems that extract and process voice, text, video and metadata.



NSA collects, identifies, sorts and stores at least 11 different types of electronic communications

What the analyst sees

For example, a completed PRISM search may yield e-mails, login credentials, metadata, stored files and videos. After processing, they are automatically sent to the analyst who made the original tasking. The time elapsed from tasking to response is thought to range from minutes to hours. A senior intelligence official would say only, "Much though we might wish otherwise, the latency is not zero."



Checks and balances

The program as a whole is authorized once a year in a secret order from the Foreign Intelligence Surveillance Court. There are no individual warrants, even for access to full content.

Before an analyst may conduct live surveillance using PRISM, a second analyst in his subject area must concur. In this "validation" process, the second analyst confirms that the surveillance has a valid foreign-intelligence purpose, that there is a "reasonable belief" that the target is neither American nor on U.S. territory, and that the surveillance complies with NSA regulations and the classified judicial order interpreting Section 702 of the FISA Amendments Act.

For stored content, a similar review takes place in the NSA's office of Standards and Compliance. There is a second review by the FBI to ensure that the target does not match a U.S. citizen or U.S. resident in FBI files.

OTHER SPY PROGRAMS

Most "metadata," or records of the people, locations, equipment, times, dates and durations of communications, are collected in programs other than PRISM. Some come from what NSA calls Upstream: interception at the biggest junctions of the internet and telephone networks. Others come directly from telephone companies – AT&T, Verizon Business Services and Sprint – who keep detailed calling records.

Information collected on Americans

If a target turns out to be an American or a person located in the United States, the NSA calls the collection "inadvertent" and usually destroys the results. If the target is foreign but the search results include U.S. communications, the NSA calls this "incidental" collection and generally keeps the U.S. content for five years. There are "minimization" rules to limit the use and distribution of the communications of identifiable U.S. citizens or residents. The NSA discloses the identities to other agencies if it believes there is evidence of a crime or that the identities are essential to understanding an intelligence report.