The Washington Post

SUNDAY, JUNE 16, 2013

NSA SURVEILLANCE

# THE ARCHITECTURE

## Four-pronged U.S. approach relies heavily on data behind Internet, phone communications

**By Barton Gellman**

On March 12, 2004, acting attorney general James B. Comey and the Justice Department's top leadership reached the brink of resignation over electronic surveillance orders that they believed to be illegal.

President George W. Bush backed down, halting secret foreign-intelligence-gathering operations that had crossed into domestic terrain. That morning marked the beginning of the end of STELLARWIND, the cover name for a set of four surveillance programs that brought Americans and American territory within the domain of the National Security Agency for the first time in decades. It was also a prelude to new legal structures that allowed Bush and then President Obama to reproduce each of those programs and expand their reach.

What exactly STELLARWIND did has never been disclosed in an unclassified form. Which parts of it did Comey approve? Which did he shut down? What became of the programs when the crisis passed and Comey, now Obama's expected nominee for FBI director, returned to private life?

Authoritative new answers to those questions, drawing upon a classified NSA history of STELLARWIND and interviews with high-ranking intelligence officials, offer the clearest map yet of the Bush-era

CONNIE ZHOU/GOOGLE VIA ASSOCIATI


**MAINWAY**
telephone metadata


**MARINA**
Internet metadata

**NUCLEON**
contents of phone calls

**PRISM**
contents of Interr communications

Above, a campus-network room at a Google data center in Council Bluffs, Iowa. The PRISM project, one of the National Security Agency's four major lines of intelligence collection, draws data held by Google, Yahoo, Microsoft and other Silicon Valley giants.

programs and the NSA's contemporary U.S. operations.

STELLARWIND was succeeded by four major lines of intelligence collection in the territorial United States, together capable of spanning the full range of modern telecommunications, according to the interviews and documents.

Foreigners, not Americans, are the NSA's "targets," as the law defines that term. But the programs are structured broadly enough that they touch nearly every American household in some way. Obama administration officials and career intelligence officers say Americans should take comfort that privacy protections are built into the design and oversight, but they are not prepared to discuss the details.

The White House, the NSA and the Office of the Director of National Intelligence declined to comment on the record for this article. A senior intelligence official agreed to answer questions if not identified.

"We have rich oversight across three branches of government. I've got an [inspector general] here, a fairly robust legal staff here … and there's the Justice Department's national security division," the official said. "For those things done under court jurisdiction, the courts are intrusive in my business, appropriately so, and there are two congressional committees. It's a belts-and-suspenders-and-Velcro approach, and inside there's rich auditing."

But privacy advocates, such as Sen. Ron Wyden (D-Ore.), said the intelligence committee on which he serves needs "straight answers" to do vigorous oversight.

He added: "The typical person says, 'If I am law-abiding and the government is out there collecting lots of information about me — who I call, when I call, where I call from' … I think the typical person is going to say, 'That sure sounds like it could have some effect on my privacy.'"

Two of the four collection programs, one each for telephony and the Internet, process trillions of "metadata" records for storage and analysis in systems called MAINWAY and MARINA, respectively. Metadata includes highly revealing information about the times, places, devices and participants in electronic communication, but not its contents. The bulk collection of telephone call records from Verizon Business Services, disclosed this month by the British newspaper the Guardian, is one source of raw intelligence for MAINWAY.

The other two types of collection, which operate on a much smaller scale, are aimed at content. One of them intercepts telephone calls and routes the spoken words to a system called NUCLEON.

For Internet content, the most important source collection is the PRISM project reported on June 6 by The Washington Post and the Guardian. It draws from data held by Google, Yahoo, Microsoft and other Silicon Valley giants, collectively the richest depositories of personal information in history.

Former NSA contractor Edward Snowden, 29, who unmasked himself as the source behind the PRISM and Verizon revelations, said he hoped for a systematic debate about the "danger to our freedom and way of life" posed by a surveillance apparatus "kept in check by nothing more than policy."

For well over a week, he has had his wish. Startling disclosures have poured out of the nation's largest and arguably tightest-lipped spy agency at an unprecedented pace. Snowden's disclosures have opened a national conversation about the limits of secret surveillance in a free society and an outcry overseas against U.S. espionage.

The debate has focused on two of the four U.S.-based collection programs: PRISM, for Internet content, and the comprehensive collection of telephone call records, foreign and domestic, that the Guardian revealed by posting a classified order from the Foreign Intelligence Surveillance Court to Verizon Business Services.

The Post has learned that similar orders have been renewed every three months for other large U.S. phone companies, including Bell South and AT&T, since May 24, 2006. On that day, the surveillance court made a fundamental shift in its approach to Section 215 of the Patriot Act,


KEVIN LAMARQUE/REUTERS

**ABOVE: Bush administration officials James Comey, left, acting attorney general for a time, and Jack Goldsmith, right, of the Office of Legal Counsel.**

**TOP: President George W. Bush in 2008 at the National Security Agency at Fort Meade. From left are Vice President Dick Cheney, NSA Director Keith Alexander and, at right, Mike McConnell, then the director of national intelligence.**

**RIGHT: Protesters listen to McConnell speak during testimony before a Senate panel in 2007.**


KEN CEDENO/BLOOMBERG NEWS

which permits the FBI to compel production of "business records" that are relevant to a particular terrorism investigation and to share those in some circumstances with the NSA. Henceforth, the court ruled, it would define the relevant business records as the entirety of a telephone company's call database.

The Bush administration, by then, had been taking "bulk metadata" from the phone companies under voluntary agreements for more than four years. The volume of information overwhelmed the MAINWAY database, according to a classified report from the NSA inspector general in 2009. The agency spent $146 million in supplemental counterterrorism funds to buy new hardware and contract support — and to make unspecified payments to the phone companies for "collaborative partnerships."

When the New York Times revealed the warrantless surveillance of voice calls, in December 2005, the telephone companies got nervous. One of them, unnamed

in the report, approached the NSA with a request. Rather than volunteer the data, at a price, the "provider preferred to be compelled to do so by a court order," the report said. Other companies followed suit. The surveillance court order that recast the meaning of business records "essentially gave NSA the same authority to collect bulk telephony metadata from business records that it had" under Bush's asserted authority alone.

Telephone metadata was not the issue that sparked a rebellion at the Justice Department, first by Jack Goldsmith of the Office of Legal Counsel and then by Comey, who was acting attorney general because John D. Ashcroft was in intensive care with acute gallstone pancreatitis. It was Internet metadata.

At Bush's direction, in orders prepared by David Addington, the counsel to Vice President Richard B. Cheney, the NSA had been siphoning e-mail metadata and technical records of Skype calls from data links owned by AT&T, Sprint and MCI, which later merged with Verizon.

For reasons unspecified in the report, Goldsmith and Comey became convinced that Bush had no lawful authority to do that.

MARINA and the collection tools that feed it are probably the least known of the NSA's domestic operations, even among experts who follow the subject closely. Yet they probably capture information about more American citizens than any other, because the volume of e-mail, chats and other Internet communications far exceeds the volume of standard telephone calls.

The NSA calls Internet metadata "digital network information." Sophisticated analysis of those records can reveal unknown associates of known terrorism suspects. Depending on the methods applied, it can also expose medical conditions, political or religious affiliations, confidential business negotiations and extramarital affairs.

What permits the former and prevents the latter is a complex set of policies that the public is not permitted to see. "You could do analyses that give you more information, but the law and procedures don't allow that," a senior U.S. intelligence lawyer said.

In the urgent aftermath of Sept. 11, 2001, with more attacks thought to be imminent, analysts wanted to use "contact chaining" techniques to build what the NSA describes as network graphs of people who represented potential threats.

The legal challenge for the NSA was that its practice of collecting high volumes of data from digital links did not seem to meet even the relatively low requirements of Bush's authorization, which allowed collection of Internet metadata "for communications with at least one communicant outside the United States or for which no communicant was known to be a citizen of the United States," the NSA inspector general's report said.

Lawyers for the agency came up with an interpretation that said the NSA did not "acquire" the communications, a term with formal meaning in surveillance law, until analysts ran searches against it. The NSA could "obtain" metadata in bulk, they argued, without meeting the required standards for acquisition.

Goldsmith and Comey did not buy that argument, and a high-ranking U.S. intelligence official said the NSA does not rely on it today.

As soon as surveillance data "touches us, we've got it, whatever verbs you choose to use," the official said in an interview. "We're not saying there's a magic formula that lets us have it without having it."

When Comey finally ordered a stop to the program, Bush signed an order renewing it anyway. Comey, Goldsmith, FBI Director Robert S. Mueller III and most of the senior Bush appointees in the Justice Department began drafting letters of resignation.

Then-NSA Director Michael V. Hayden was not among them. According to the inspector general's classified report, Cheney's lawyer, Addington, placed a phone call and "General Hayden had to decide whether NSA would execute the Authorization

without the Attorney General's signature." He decided to go along.

The following morning, when Mueller told Bush that he and Comey intended to resign, the president reversed himself.

Three months later, on July 15, the secret surveillance court allowed the NSA to resume bulk collection under the court's own authority. The opinion, which remains highly classified, was based on a provision of electronic surveillance law, known as "pen register, trap and trace," that was written to allow law enforcement officers to obtain the phone numbers of incoming and outgoing calls from a single telephone line.

When the NSA aims for foreign targets whose communications cross U.S. infrastructure, it expects to sweep in some American content "incidentally" or "inadvertently," which are terms of art in regulations governing the NSA. Contact chaining, because it extends to the contacts of contacts of targets, inevitably collects even more American data.

Current NSA director Keith B. Alexander and Director of National Intelligence James R. Clapper Jr. have resolutely refused to offer an estimate of the number of Americans whose calls or e-mails have thus made their way into content databases such as NUCLEON.

The agency and its advocates maintain that its protection of that data is subject to rigorous controls and oversight by Congress and courts. For the public, it comes down to a question of unverifiable trust.

"The constraints that I operate under are much more remarkable than the powers that I enjoy," said the senior intelligence official who declined to be named.

When asked why the NSA could not release an unclassified copy of its "minimization procedures," which are supposed to strip accidentally collected records of their identifying details, the official suggested a reporter submit a freedom-of-information request.

As for bulk collection of Internet metadata, the question that triggered the crisis of 2004, another official said the NSA is no longer doing it. When pressed on that question, he said he was speaking only of collections under authority of the surveillance court.

"I'm not going to say we're not collecting any Internet metadata," he added. "We're not using this program and these kinds of accesses to collect Internet metadata in bulk."

*bart.gellman@washpost.com*

---

Julie Tate and Ellen Nakashima contributed to this report.