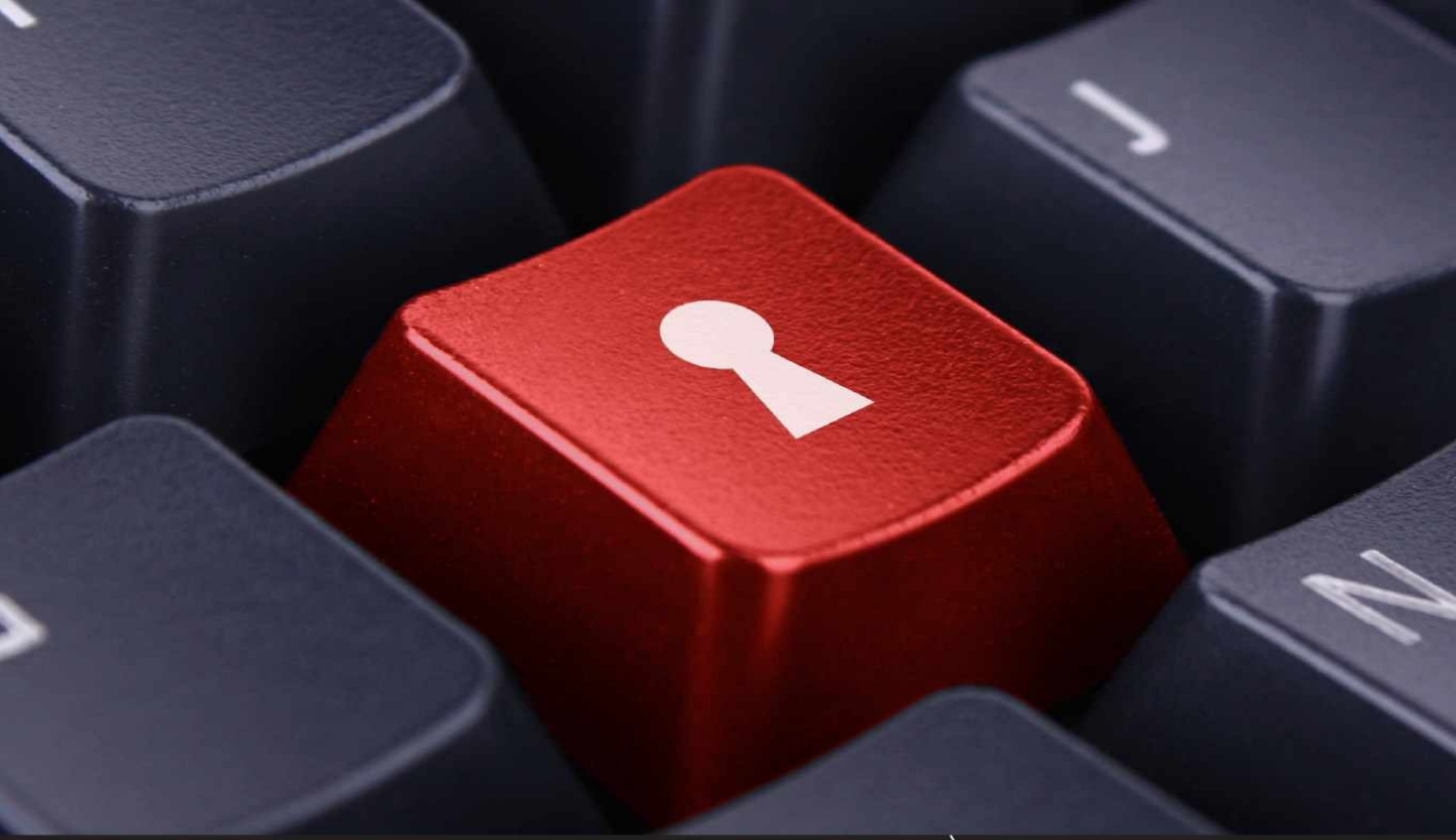

The Washington Post E·BOOK

NSA SECRETS

GOVERNMENT SPYING IN THE INTERNET AGE

Table of Contents

- NSA Secrets
- Copyright
- Introduction
- U.S., British intelligence mining data from nine U.S. Internet companies in broad secr program
- From obscurity to notoriety, Snowden took an unusual path
- Edward Snowden, Bradley Manning and the risk of the low-level, tech-savvy leaker
- U.S. surveillance architecture includes collection of revealing Internet, phone metadata
- Metadata reveals secrets of social position, company hierarchy, terrorist cells
- New documents reveal parameters of NSA's secret surveillance programs
- President's surveillance program worked with private sector to collect data after Sept. 11, 2001
- For NSA chief, terrorist threat drives passion to 'collect it all, observers say
- NSA broke privacy rules thousands of times per year, audit finds
- FISA court: Ability to police U.S. spying program limited
- NSA gathered thousands of Americans' e-mails before court ordered it to revise its tactics
- U.S. spy network's successes, failures and objectives detailed in 'black budget' summary
- NSA paying U.S. companies for access to communications networks
- To hunt Osama bin Laden, satellites watched over Abbottabad, Pakistan, and Navy SEALs
- U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show
- Spy agencies spend millions to hunt for insider threats, document shows
- Top-secret files show new levels of distrust of Pakistan
- U.S. documents detail al-Qaeda's efforts to fight back against drones
- Obama administration had NSA restrictions reversed in 2011
- Declassified court documents highlight NSA violations in data collection
- FISA court releases opinion upholding NSA phone program
- U.S. officials dodge questions on scope of surveillance
- NSA report on the Tor Encrypted Network
- Dual-leadership role at NSA and Cyber Command stirs debate
- NSA tries to regain industry's trust to work cooperatively against cyber-threats
- Effort underway to declassify document that is legal foundation for NSA phone program
- NSA collects millions of e-mail address books globally
- Documents reveal NSA's extensive involvement in targeted killing program
- NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say
- NSA tracking cellphone locations worldwide, Snowden documents show
- Judge: NSA's collecting of phone records is probably unconstitutional

- More from the Washington Post
- Connect with Diversion Books

NSA Secrets

Government Spying in the Internet Age

The Washington Post

Copyright

Diversion Books
A Division of Diversion Publishing Corp.
443 Park Avenue South, Suite 1004
New York, New York 10016

www.DiversionBooks.com

For more information, email info@diversionbooks.com

First Diversion Books edition December 2013

ISBN: 978-1-62681-212-3

Introduction

By Barton Gellman
December 23, 2013

An undated handout photo by the National Security Agency (NSA) shows the NSA headquarters in Fort Meade, Maryland, USA. secret intelligence program called 'Prism' run by the NSA has been collecting data from millions of communication servi subscribers through access to many of the top Internet companies, including Google, Facebook, Apple and Verizon. (*EPA/Natior Security Agency/Handout*)

MOSCOW — The familiar voice on the hotel room phone did not waste words.

"What time does your clock say, exactly?" he asked.

He checked the reply against his watch and described a place to meet.

"I'll see you there," he said.

Edward Joseph Snowden emerged at the appointed hour, alone, blending into a light crowd locals and tourists. He cocked his arm for a handshake, then turned his shoulder to indicate a pat

Before long he had guided his visitor to a secure space out of public view.

During more than 14 hours of interviews, the first he has conducted in person since arriving he in June, Snowden did not part the curtains or step outside. Russia granted him temporary asylum o Aug. 1, but Snowden remains a target of surpassing interest to the intelligence services whose secre he spilled on an epic scale.

Late this spring, Snowden supplied three journalists, including this one, with caches of top-secr documents from the National Security Agency, where he worked as a contractor. Dozens o revelations followed, and then hundreds, as news organizations around the world picked up the stor Congress pressed for explanations, new evidence revived old lawsuits and the Obama administratio was obliged to declassify thousands of pages it had fought for years to conceal.

Taken together, the revelations have brought to light a global surveillance system that cast o many of its historical restraints after the attacks of Sept. 11, 2001. Secret legal authorities empowere the NSA to sweep in the telephone, Internet and location records of whole populations. One of th leaked presentation slides described the agency's "collection philosophy" as "Order one of everythin off the menu."

Six months after the first revelations appeared in The Washington Post and Britain's Guardia newspaper, Snowden agreed to reflect at length on the roots and repercussions of his choice. He wa relaxed and animated over two days of nearly unbroken conversation, fueled by burgers, pasta, ic cream and Russian pastry.

Snowden offered vignettes from his intelligence career and from his recent life as "an indoor ca in Russia. But he consistently steered the conversation back to surveillance, democracy and th meaning of the documents he exposed.

"For me, in terms of personal satisfaction, the mission's already accomplished," he said. already won. As soon as the journalists were able to work, everything that I had been trying to do wa validated. Because, remember, I didn't want to change society. I wanted to give society a chance t determine if it should change itself."

"All I wanted was for the public to be able to have a say in how they are governed," he said. "Th is a milestone we left a long time ago. Right now, all we are looking at are stretch goals."

'Going in blind'

Snowden is an orderly thinker, with an engineer's approach to problem-solving. He had come t believe that a dangerous machine of mass surveillance was growing unchecked. Closed-door oversig by Congress and the Foreign Intelligence Surveillance Court was a "graveyard of judgment," he sai manipulated by the agency it was supposed to keep in check. Classification rules erected walls prevent public debate.

Toppling those walls would be a spectacular act of transgression against the norms that prevaile inside them. Someone would have to bypass security, extract the secrets, make undetected conta with journalists and provide them with enough proof to tell the stories.

The NSA's business is "information dominance," the use of other people's secrets to shape event At 29, Snowden upended the agency on its own turf.

"You recognize that you're going in blind, that there's no model," Snowden said, acknowledgin that he had no way to know whether the public would share his views.

"But when you weigh that against the alternative, which is not to act," he said, "you realize th some analysis is better than no analysis. Because even if your analysis proves to be wrong, t marketplace of ideas will bear that out. If you look at it from an engineering perspective, an iterati perspective, it's clear that you have to try something rather than do nothing."

By his own terms, Snowden succeeded beyond plausible ambition. The NSA, accustomed watching without being watched, faces scrutiny it has not endured since the 1970s, or perhaps ever.

The cascading effects have made themselves felt in Congress, the courts, popular culture, Silic Valley and world capitals. The basic structure of the Internet itself is now in question, as Brazil ar members of the European Union consider measures to keep their data away from U.S. territory ar U.S. technology giants including Google, Microsoft and Yahoo take extraordinary steps to block th collection of data by their government.

For months, Obama administration officials attacked Snowden's motives and said the work of th NSA was distorted by selective leaks and misinterpretations.

On Dec. 16, in a lawsuit that could not have gone forward without the disclosures made possib by Snowden, U.S. District Judge Richard J. Leon described the NSA's capabilities as "almo Orwellian" and said its bulk collection of U.S. domestic telephone records was probab unconstitutional.

The next day, in the Roosevelt Room, an unusual delegation of executives from old telepho companies and young Internet firms told President Obama that the NSA's intrusion into the networks was a threat to the U.S. information economy. The following day, an advisory pan appointed by Obama recommended substantial new restrictions on the NSA, including an end to t domestic call-records program.

"This week is a turning point," said the Government Accountability Project's Jesselyn Radac who is one of Snowden's legal advisers. "It has been just a cascade."

'They elected me'

On June 22, the Justice Department unsealed a criminal complaint charging Snowden wi espionage and felony theft of government property. It was a dry enumeration of statutes, without

trace of the anger pulsing through Snowden's former precincts.

In the intelligence and national security establishments, Snowden is widely viewed as a reckle saboteur, and journalists abetting him little less so.

At the Aspen Security Forum in July, a four-star military officer known for his even keel seethe through one meeting alongside a reporter he knew to be in contact with Snowden. Before walkin away, he turned and pointed a finger.

"We didn't have another 9/11," he said angrily, because intelligence enabled warfighters to fin the enemy first. "Until you've got to pull the trigger, until you've had to bury your people, you don have a clue."

It is commonly said of Snowden that he broke an oath of secrecy, a turn of phrase that captures sense of betrayal. NSA Director Keith B. Alexander and Director of National Intelligence James R Clapper Jr., among many others, have used that formula.

In his interview with The Post, Snowden noted matter-of-factly that Standard Form 312, th classified-information nondisclosure agreement, is a civil contract. He signed it, but he pledged h fealty elsewhere.

"The oath of allegiance is not an oath of secrecy," he said. "That is an oath to the Constitutio That is the oath that I kept that Keith Alexander and James Clapper did not."

People who accuse him of disloyalty, he said, mistake his purpose.

"I am not trying to bring down the NSA, I am working to improve the NSA," he said. "I am str working for the NSA right now. They are the only ones who don't realize it."

What entitled Snowden, now 30, to take on that responsibility?

"That whole question — who elected you? — inverts the model," he said. "They elected me. Th overseers."

He named the chairmen of the Senate and House intelligence committees.

"Dianne Feinstein elected me when she asked softball questions" in committee hearings, he sai "Mike Rogers elected me when he kept these programs hidden. … The FISA court elected me whe they decided to legislate from the bench on things that were far beyond the mandate of what that cou was ever intended to do. The system failed comprehensively, and each level of oversight, each level responsibility that should have addressed this, abdicated their responsibility."

"It wasn't that they put it on me as an individual — that I'm uniquely qualified, an ang descending from the heavens — as that they put it on someone, somewhere," he said. "You have th capability, and you realize every other [person] sitting around the table has the same capability b they don't do it. So somebody has to be the first."

'Front-page test'

Snowden grants that NSA employees by and large believe in their mission and trust the agency t
handle the secrets it takes from ordinary people — deliberately, in the case of bulk records collectio
and "incidentally," when the content of American phone calls and e-mails are swept into NSA system
along with foreign targets.

But Snowden also said acceptance of the agency's operations was not universal. He began to te
that proposition more than a year ago, he said, in periodic conversations with co-workers an
superiors that foreshadowed his emerging plan.

Beginning in October 2012, he said, he brought his misgivings to two superiors in the NSA
Technology Directorate and two more in the NSA Threat Operations Center's regional base in Hawai
For each of them, and 15 other co-workers, Snowden said he opened a data query tool calle
BOUNDLESSINFORMANT, which used color-coded "heat maps" to depict the volume of da
ingested by NSA taps.

His colleagues were often "astonished to learn we are collecting more in the United States o
Americans than we are on Russians in Russia," he said. Many of them were troubled, he said, an
several said they did not want to know any more.

"I asked these people, 'What do you think the public would do if this was on the front page?' " h
said. He noted that critics have accused him of bypassing internal channels of dissent. "How is that n
reporting it? How is that not raising it?" he said.

By last December, Snowden was contacting reporters, although he had not yet passed along an
classified information. He continued to give his colleagues the "front-page test," he said, until April.

Asked about those conversations, NSA spokeswoman Vanee Vines sent a prepared statement t
The Post: "After extensive investigation, including interviews with his former NSA supervisors an
co-workers, we have not found any evidence to support Mr. Snowden's contention that he brough
these matters to anyone's attention."

Snowden recounted another set of conversations that he said took place three years earlier, whe
he was sent by the NSA's Technology Directorate to support operations at a listening post in Japan. A
a system administrator, he had full access to security and auditing controls. He said he saw seriou
flaws with information security.

"I actually recommended they move to two-man control for administrative access back in 2009
he said, first to his supervisor in Japan and then to the directorate's chief of operations in the Pacifi
"Sure, a whistleblower could use these things, but so could a spy."

That precaution, which requires a second set of credentials to perform risky operations such
copying files onto a removable drive, has been among the principal security responses to the Snowde
affair.

Vines, the NSA spokeswoman, said there was no record of those conversations, either.

U.S. 'would cease to exist'

Just before releasing the documents this spring, Snowden made a final review of the risks. He ha overcome what he described at the time as a "selfish fear" of the consequences for himself.

"I said to you the only fear [left] is apathy — that people won't care, that they won't wa change," he recalled this month.

The documents leaked by Snowden compelled attention because they revealed to Americans history they did not know they had.

Internal briefing documents reveled in the "Golden Age of Electronic Surveillance." Brawny cov names such as MUSCULAR, TUMULT and TURMOIL boasted of the agency's prowess.

With assistance from private communications firms, the NSA had learned to capture enormou flows of data at the speed of light from fiber-optic cables that carried Internet and telephone traff over continents and under seas. According to one document in Snowden's cache, the agency's Speci Source Operations group, which as early as 2006 was said to be ingesting "one Library of Congre every 14.4 seconds," had an official seal that might have been parody: an eagle with all the world cables in its grasp.

Each year, NSA systems collected hundreds of millions of e-mail address books, hundreds billions of cellphone location records and trillions of domestic call logs.

Most of that data, by definition and intent, belonged to ordinary people suspected of nothing. B vast new storage capacity and processing tools enabled the NSA to use the information to map huma relationships on a planetary scale. Only this way, its leadership believed, could the NSA reach beyon its universe of known intelligence targets.

In the view of the NSA, signals intelligence, or electronic eavesdropping, was a matter of life an death, "without which America would cease to exist as we know it," according to an intern presentation in the first week of October 2001 as the agency ramped up its response to the al-Qae attacks on the World Trade Center and the Pentagon.

With stakes such as those, there was no capability the NSA believed it should leave on the tabl The agency followed orders from President George W. Bush to begin domestic collection witho authority from Congress and the courts. When the NSA won those authorities later, some of the under secret interpretations of laws passed by Congress between 2007 and 2012, the Oban administration went further still.

Using PRISM, the cover name for collection of user data from Google, Yahoo, Microsoft, Appl and five other U.S.-based companies, the NSA could obtain all communications to or from an specified target. The companies had no choice but to comply with the government's request for data.

But the NSA could not use PRISM, which was overseen once a year by the surveillance court, f the collection of virtually all data handled by those companies. To widen its access, it teamed up wi its British counterpart, Government Communications Headquarters, or GCHQ, to break into th

private fiber-optic links that connected Google and Yahoo data centers around the world.

That operation, which used the cover name MUSCULAR, tapped into U.S. company data fro outside U.S. territory. The NSA, therefore, believed it did not need permission from Congress judicial oversight. Data from hundreds of millions of U.S. accounts flowed over those Google a Yahoo links, but classified rules allowed the NSA to presume that data ingested overseas belonged foreigners.

‘Persistent threat’

Disclosure of the MUSCULAR project enraged and galvanized U.S. technology executives. Th believed the NSA had lawful access to their front doors — and had broken down the back doo anyway.

Microsoft general counsel Brad Smith took to his company’s blog and called the NSA “advanced persistent threat” — the worst of all fighting words in U.S. cybersecurity circles, general reserved for Chinese state-sponsored hackers and sophisticated criminal enterprises.

“For the industry as a whole, it caused everyone to ask whether we knew as much as we thought Smith recalled in an interview. “It underscored the fact that while people were confident that the U. government was complying with U.S. laws for activity within U.S. territory, perhaps there were thing going on outside the United States … that made this bigger and more complicated and mo disconcerting than we knew.”

They wondered, he said, whether the NSA was “collecting proprietary information from th companies themselves.”

Led by Google and then Yahoo, one company after another announced expensive plans to encry its data traffic over tens of thousands of miles of cable. It was a direct — in some cases, explicit blow to NSA collection of user data in bulk. If the NSA wanted the information, it would have request it or circumvent the encryption one target at a time.

As these projects are completed, the Internet will become a less friendly place for the NSA work. The agency can still collect data from virtually anyone, but collecting from everyone will harder.

The industry’s response, Smith acknowledged, was driven by a business threat. U.S. compani could not afford to be seen as candy stores for U.S. intelligence. But the principle of the thing, Smi said, “is fundamentally about ensuring that customer data is turned over to governments pursuant valid legal orders and in accordance with constitutional principles.”

‘Warheads on foreheads’

Snowden has focused on much the same point from the beginning: Individual targeting would cu

most of what he believes is wrong with the NSA.

Six months ago, a reporter asked him by encrypted e-mail why Americans would want the NSA t
give up bulk data collection if that would limit a useful intelligence tool.

“I believe the cost of frank public debate about the powers of our government is less than th
danger posed by allowing these powers to continue growing in secret,” he replied, calling them
direct threat to democratic governance.”

In the Moscow interview, Snowden said, “What the government wants is something they never ha
before,” adding: “They want total awareness. The question is, is that something we should l
allowing?”

Snowden likened the NSA’s powers to those used by British authorities in Colonial America, whe
“general warrants” allowed for anyone to be searched. The FISA court, Snowden said, “is authorizin
general warrants for the entire country’s metadata.”

“The last time that happened, we fought a war over it,” he said.

Technology, of course, has enabled a great deal of consumer surveillance by private companies, a
well. The difference with the NSA’s possession of the data, Snowden said, is that government has th
power to take away life or freedom.

At the NSA, he said, “there are people in the office who joke about, ‘We put warheads o
foreheads.’ Twitter doesn’t put warheads on foreheads.”

Privacy, as Snowden sees it, is a universal right, applicable to American and foreign surveillanc
alike.

“I don’t care whether you’re the pope or Osama bin Laden,” he said. “As long as there’s a
individualized, articulable, probable cause for targeting these people as legitimate foreig
intelligence, that’s fine. I don’t think it’s imposing a ridiculous burden by asking for probable caus
Because, you have to understand, when you have access to the tools the NSA does, probable caus
falls out of trees.”

‘Everybody knows’

On June 29, Gilles de Kerchove, the European Union’s counterterrorism coordinator, awoke to
report in Der Spiegel that U.S. intelligence had broken into E.U. offices, including his, to impla
surveillance devices.

The 56-year-old Belgian, whose work is often classified, did not consider himself naive. But h
took the news personally, and more so when he heard unofficial explanations from Washington.

“ ‘Everybody knows. Everybody does’ — Keith Alexander said that,” de Kerchove said in a
interview. “I don’t like the idea that the NSA will put bugs in my office. No. I don’t like it. N

Between allies? No. I'm surprised that people find that noble."

Comparable reactions, expressed less politely in private, accompanied revelations that the NS had tapped the cellphones of German Chancellor Angela Merkel and Brazilian President Dilm Rousseff. The blowback roiled relations with both allies, among others. Rousseff canceled a sta dinner with Obama in September.

When it comes to spying on allies, by Snowden's lights, the news is not always about the target.

"It's the deception of the government that's revealed," Snowden said, noting that the Obam administration offered false public assurances after the initial reports about NSA surveillance Germany "The U.S. government said: 'We follow German laws in Germany. We never target Germa citizens.' And then the story comes out and it's: 'What are you talking about? You're spying on th chancellor.' You just lied to the entire country, in front of Congress."

In private, U.S. intelligence officials still maintain that spying among friends is routine for a concerned, but they are giving greater weight to the risk of getting caught.

"There are many things we do in intelligence that, if revealed, would have the potential for a kinds of blowback," Clapper told a House panel in October.

'They will make mistakes'

U.S. officials say it is obvious that Snowden's disclosures will do grave harm to intelligen gathering, exposing methods that adversaries will learn to avoid.

"We're seeing al-Qaeda and related groups start to look for ways to adjust how the communicate," said Matthew Olsen, director of the National Counterterrorism Center and a form general counsel at the NSA.

Other officials, who declined to speak on the record about particulars, said they had watched son of their surveillance targets, in effect, changing channels. That evidence can be read another way, the acknowledged, given that the NSA managed to monitor the shift.

Clapper has said repeatedly in public that the leaks did great damage, but in private he has taken more nuanced stance. A review of early damage assessments in previous espionage cases, he said one closed-door briefing this fall, found that dire forecasts of harm were seldom borne out.

"People must communicate," he said, according to one participant who described the confidenti meeting on the condition of anonymity. "They will make mistakes, and we will exploit them."

According to senior intelligence officials, two uncertainties feed their greatest concerns. One whether Russia or China managed to take the Snowden archive from his computer, a worst-cas assumption for which three officials acknowledged there is no evidence.

In a previous assignment, Snowden taught U.S. intelligence personnel how to operate securely in "high-threat digital environment," using a training scenario in which China was the designated threa

He declined to discuss the whereabouts of the files, but he said that he is confident he did not expo
them to Chinese intelligence in Hong Kong. And he said he did not bring them to Russia.

"There's nothing on it," he said, turning his laptop screen toward his visitor. "My hard drive
completely blank."

The other big question is how many documents Snowden took. The NSA's incoming deput
director, Rick Ledgett, said on CBS's "60 Minutes" recently that the number may approach 1
million, a huge and unexplained spike over previous estimates. Ledgett said he would favor trying
negotiate an amnesty with Snowden in exchange for "assurances that the remainder of the data cou
be secured."

Obama's national security adviser, Susan E. Rice, later dismissed the possibility.

"The government knows where to find us if they want to have a productive conversation abo
resolutions that don't involve Edward Snowden behind bars," said the American Civil Liberti
Union's Ben Wizner, the central figure on Snowden's legal team.

Some news accounts have quoted U.S. government officials as saying Snowden has arranged f
the automated release of sensitive documents if he is arrested or harmed. There are strong reasons
doubt that, beginning with Snowden's insistence, to this reporter and others, that he does not want th
documents published in bulk.

If Snowden were fool enough to rig a "dead man's switch," confidants said, he would be invitin
anyone who wants the documents to kill him.

Asked about such a mechanism in the Moscow interview, Snowden made a face and declined
reply. Later, he sent an encrypted message. "That sounds more like a suicide switch," he wrote. "
wouldn't make sense."

'It's not about me'

By temperament and circumstance, Snowden is a reticent man, reluctant to discuss details abo
his personal life.

Over two days his guard never dropped, but he allowed a few fragments to emerge. He is a
"ascetic," he said. He lives off ramen noodles and chips. He has visitors, and many of them brin
books. The books pile up, unread. The Internet is an endless library and a window on the progress
his cause.

"It has always been really difficult to get me to leave the house," he said. "I just don't have a lot
needs. … Occasionally there's things to go do, things to go see, people to meet, tasks to accomplis
But it's really got to be goal-oriented, you know. Otherwise, as long as I can sit down and think an
write and talk to somebody, that's more meaningful to me than going out and looking at landmarks."

In hope of keeping focus on the NSA, Snowden has ignored attacks on himself.

“Let them say what they want,” he said. “It’s not about me.”

Former NSA and CIA director Michael V. Hayden predicted that Snowden will waste away i Moscow as an alcoholic, like other “defectors.” To this, Snowden shrugged. He does not drink at a Never has.

But Snowden knows his presence here is easy ammunition for critics. He did not choose refuge Moscow as a final destination. He said that once the U.S. government voided his passport as he tri to change planes en route to Latin America, he had no other choice.

It would be odd if Russian authorities did not keep an eye on him, but no retinue accompani Snowden and his visitor saw no one else nearby. Snowden neither tried to communicate furtively n asked that his visitor do so. He has had continuous Internet access and has talked to his attorneys a to journalists daily, from his first day in the transit lounge at Sheremetyevo airport.

“There is no evidence at all for the claim that I have loyalties to Russia or China or any count other than the United States,” he said. “I have no relationship with the Russian government. I have n entered into any agreements with them.”

“If I defected at all,” Snowden said, “I defected from the government to the public.”

Julie Tate contributed to this report.

U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program

By Barton Gellman and Laura Poitras
June 6, 2013

The National Security Agency and the FBI are tapping directly into the central servers of nine leadi U.S. Internet companies, extracting audio and video chats, photographs, e-mails, documents, a connection logs that enable analysts to track foreign targets, according to a top-secret docume obtained by The Washington Post.

The program, code-named PRISM, has not been made public until now. It may be the first of i kind. The NSA prides itself on stealing secrets and breaking codes, and it is accustomed to corpora partnerships that help it divert data traffic or sidestep barriers. But there has never been a Google Facebook before, and it is unlikely that there are richer troves of valuable intelligence than the ones Silicon Valley.

Equally unusual is the way the NSA extracts what it wants, according to the document: "Collecti directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google, Faceboo PalTalk, AOL, Skype, YouTube, Apple."

London's Guardian newspaper reported Friday that GCHQ, Britain's equivalent of the NSA, als has been secretly gathering intelligence from the same internet companies through an operation set u by the NSA.

According to documents obtained by The Guardian, PRISM would appear to allow GCHQ circumvent the formal legal process required in Britain to seek personal material such as email photos and videos from an internet company based outside of the country.

PRISM was launched from the ashes of President George W. Bush's secret program of warrantles domestic surveillance in 2007, after news media disclosures, lawsuits and the Foreign Intelligen Surveillance Court forced the president to look for new authority.

Congress obliged with the Protect America Act in 2007 and the FISA Amendments Act of 2008 which immunized private companies that cooperated voluntarily with U.S. intelligence collectio PRISM recruited its first partner, Microsoft, and began six years of rapidly growing data collecti beneath the surface of a roiling national debate on surveillance and privacy. Late last year, whe critics in Congress sought changes in the FISA Amendments Act, the only lawmakers who knew abou

PRISM were bound by oaths of office to hold their tongues.

The court-approved program is focused on foreign communications traffic, which often flo through U.S. servers even when sent from one overseas location to another. Between 2004 and 200 Bush administration lawyers persuaded federal FISA judges to issue surveillance orders in fundamentally new form. Until then the government had to show probable cause that a particul "target" and "facility" were both connected to terrorism or espionage.

In four new orders, which remain classified, the court defined massive data sets as "facilities" a agreed to certify periodically that the government had reasonable procedures in place to minimi collection of "U.S. persons" data without a warrant.

In a statement issue late Thursday, Director of National Intelligence James R. Clapper sa "information collected under this program is among the most important and valuable foreig intelligence information we collect, and is used to protect our nation from a wide variety of threat The unauthorized disclosure of information about this important and entirely legal program reprehensible and risks important protections for the security of Americans."

Clapper added that there were numerous inaccuracies in reports about PRISM by The Post and t Guardian newspaper, but he did not specify any.

Jameel Jaffer, deputy legal director of the American Civil Liberties Union, said: "I would ju push back on the idea that the court has signed off on it, so why worry? This is a court that meets secret, allows only the government to appear before it, and publishes almost none of its opinions. has never been an effective check on government."

Several companies contacted by The Post said they had no knowledge of the program, did n allow direct government access to their servers and asserted that they responded only to target requests for information.

"We do not provide any government organization with direct access to Facebook servers," said Jo Sullivan, chief security officer for Facebook. "When Facebook is asked for data or information abo specific individuals, we carefully scrutinize any such request for compliance with all applicable law and provide information only to the extent required by law."

"We have never heard of PRISM," said Steve Dowling, a spokesman for Apple. "We do no provide any government agency with direct access to our servers, and any government agen requesting customer data must get a court order."

It is possible that the conflict between the PRISM slides and the company spokesmen is the resu of imprecision on the part of the NSA author. In another classified report obtained by The Post, th arrangement is described as allowing "collection managers [to send] content tasking instructio directly to equipment installed at company-controlled locations," rather than directly to compa servers.

Government officials and the document itself made clear that the NSA regarded the identities

its private partners as PRISM's most sensitive secret, fearing that the companies would withdra from the program if exposed. "98 percent of PRISM production is based on Yahoo, Google an Microsoft; we need to make sure we don't harm these sources," the briefing's author wrote in h speaker's notes.

An internal presentation of 41 briefing slides on PRISM, dated April 2013 and intended for senio analysts in the NSA's Signals Intelligence Directorate, described the new tool as the most prolifi contributor to the President's Daily Brief, which cited PRISM data in 1,477 items last year. Accordin to the slides and other supporting materials obtained by The Post, "NSA reporting increasingly relie on PRISM" as its leading source of raw material, accounting for nearly 1 in 7 intelligence reports.

That is a remarkable figure in an agency that measures annual intake in the trillions communications. It is all the more striking because the NSA, whose lawful mission is foreig intelligence, is reaching deep inside the machinery of American companies that host hundreds millions of American-held accounts on American soil.

The technology companies, whose cooperation is essential to PRISM operations, include most the dominant global players of Silicon Valley, according to the document. They are listed on a roste that bears their logos in order of entry into the program: "Microsoft, Yahoo, Google, Faceboo PalTalk, AOL, Skype, YouTube, Apple." PalTalk, although much smaller, has hosted traffic o substantial intelligence interest during the Arab Spring and in the ongoing Syrian civil war.

Dropbox, the cloud storage and synchronization service, is described as "coming soon."

Sens. Ron Wyden (D-Ore.) and Mark Udall (D-Colo.), who had classified knowledge of th program as members of the Senate Intelligence Committee, were unable to speak of it when the warned in a Dec. 27, 2012, floor debate that the FISA Amendments Act had what both of them called "back-door search loophole" for the content of innocent Americans who were swept up in a search fo someone else.

"As it is written, there is nothing to prohibit the intelligence community from searching through pile of communications, which may have been incidentally or accidentally been collected without warrant, to deliberately search for the phone calls or e-mails of specific Americans," Udall said.

Wyden repeatedly asked the NSA to estimate the number of Americans whose communication had been incidentally collected, and the agency's director, Lt. Gen. Keith B. Alexander, insisted ther was no way to find out. Eventually Inspector General I. Charles McCullough III wrote Wyden a lett stating that it would violate the privacy of Americans in NSA data banks to try to estimate the number.

Roots in the '70s

PRISM is an heir, in one sense, to a history of intelligence alliances with as many as 100 truste

U.S. companies since the 1970s. The NSA calls these Special Source Operations, and PRISM fal under that rubric.

The Silicon Valley operation works alongside a parallel program, code-named BLARNEY, tha gathers up "metadata" — technical information about communications traffic and network devices - as it streams past choke points along the backbone of the Internet. BLARNEY's top-secret progra summary, set down in the slides alongside a cartoon insignia of a shamrock and a leprechaun ha describes it as "an ongoing collection program that leverages IC [intelligence community] an commercial partnerships to gain access and exploit foreign intelligence obtained from glob networks."

But the PRISM program appears to more nearly resemble the most controversial of the warrantle surveillance orders issued by President George W. Bush after the al-Qaeda attacks of Sept. 11, 200 Its history, in which President Obama presided over exponential growth in a program that candida Obama criticized, shows how fundamentally surveillance law and practice have shifted away fro individual suspicion in favor of systematic, mass collection techniques.

The Obama administration points to ongoing safeguards in the form of "extensive procedure specifically approved by the court, to ensure that only non-U.S. persons outside the U.S. are targete and that minimize the acquisition, retention and dissemination of incidentally acquired informatio about U.S. persons."

And it is true that the PRISM program is not a dragnet, exactly. From inside a company's da stream the NSA is capable of pulling out anything it likes, but under current rules the agency does n try to collect it all.

Analysts who use the system from a Web portal at Fort Meade, Md., key in "selectors," or searc terms, that are designed to produce at least 51 percent confidence in a target's "foreignness." That not a very stringent test. Training materials obtained by The Post instruct new analysts to mak quarterly reports of any accidental collection of U.S. content, but add that "it's nothing to wor about."

Even when the system works just as advertised, with no American singled out for targeting, th NSA routinely collects a great deal of American content. That is described as "incidental," and it inherent in contact chaining, one of the basic tools of the trade. To collect on a suspected spy foreign terrorist means, at minimum, that everyone in the suspect's inbox or outbox is swept i Intelligence analysts are typically taught to chain through contacts two "hops" out from their targe which increases "incidental collection" exponentially. The same math explains the aphorism, from th John Guare play, that no one is more than "six degrees of separation" from any other person.

A 'directive'

In exchange for immunity from lawsuits, companies such as Yahoo and AOL are obliged to accep
a "directive" from the attorney general and the director of national intelligence to open their servers
the FBI's Data Intercept Technology Unit, which handles liaison to U.S. companies from the NSA.
2008, Congress gave the Justice Department authority for a secret order from the Foreign Surveillan
Intelligence Court to compel a reluctant company "to comply."

In practice, there is room for a company to maneuver, delay or resist. When a clandesti
intelligence program meets a highly regulated industry, said a lawyer with experience in bridging th
gaps, neither side wants to risk a public fight. The engineering problems are so immense, in systen
of such complexity and frequent change, that the FBI and NSA would be hard pressed to build in bac
doors without active help from each company.

Apple demonstrated that resistance is possible when it held out for more than five years, f
reasons unknown, after Microsoft became PRISM's first corporate partner in May 2007. Twitte
which has cultivated a reputation for aggressive defense of its users' privacy, is still conspicuous b
its absence from the list of "private sector partners."

Google, like the other companies, denied that it permitted direct government access to its servers

"Google cares deeply about the security of our users' data," a company spokesman said. "W
disclose user data to government in accordance with the law, and we review all such reques
carefully. From time to time, people allege that we have created a government 'back door' into ou
systems, but Google does not have a 'back door' for the government to access private user data."

Microsoft also provided a statement: "We provide customer data only when we receive a legall
binding order or subpoena to do so, and never on a voluntary basis. In addition we only ever comp
with orders for requests about specific accounts or identifiers. If the government has a broad
voluntary national security program to gather customer data we don't participate in it."

Yahoo also issued a denial.

"Yahoo! takes users' privacy very seriously," the company said in a statement. "We do not provi
the government with direct access to our servers, systems, or network."

Like market researchers, but with far more privileged access, collection managers in the NSA
Special Source Operations group, which oversees the PRISM program, are drawn to the wealth
information about their subjects in online accounts. For much the same reason, civil libertarians ar
some ordinary users may be troubled by the menu available to analysts who hold the require
clearances to "task" the PRISM system.

There has been "continued exponential growth in tasking to Facebook and Skype," according to th
PRISM slides. With a few clicks and an affirmation that the subject is believed to be engaged
terrorism, espionage or nuclear proliferation, an analyst obtains full access to Facebook's "extensiv
search and surveillance capabilities against the variety of online social networking services."

According to a separate "User's Guide for PRISM Skype Collection," that service can

monitored for audio when one end of the call is a conventional telephone and for any combination
"audio, video, chat, and file transfers" when Skype users connect by computer alone. Google
offerings include Gmail, voice and video chat, Google Drive files, photo libraries, and liv
surveillance of search terms.

Firsthand experience with these systems, and horror at their capabilities, is what drove a care
intelligence officer to provide PowerPoint slides about PRISM and supporting materials to Th
Washington Post in order to expose what he believes to be a gross intrusion on privacy. "They quit
literally can watch your ideas form as you type," the officer said.

*Poitras is a documentary filmmaker and MacArthur Fellow. Julie Tate, Robert O'Harrow Jr., Cecili
Kang and Ellen Nakashima contributed to this report.*

Additional Content:

The NSA problem? Too much data.

NSA leak: Source believes exposure, consequences inevitable (VIDEO)

An excerpt from NSA's Wikipedia

From obscurity to notoriety, Snowden took an unusual path

By Ellen Nakashima
June 9, 2013

Edward Snowden said the internet “is a TV watching you.” (Photo courtesy of The Guardian)

Edward Snowden, the 29-year-old National Security Agency contractor who admitted that he wa behind recent leaks of classified intelligence, has vaulted from obscurity to international notoriet joining the ranks of high-profile leakers such as Daniel Ellsberg of Pentagon Papers fame.

The fact that Snowden stepped forward to acknowledge his leaks to The Washington Post and th Guardian newspapers rather than wait for the FBI to find him impressed others who have disclose government secrets.

“I consider it a magnificent act of civil disobedience,” said Thomas Drake, a former NSA offici who was prosecuted for leaking classified information to a journalist but wound up serving no prisc time after the government’s case fell apart. “He’s a whistleblower.”

Ellsberg was similarly impressed. He said in an interview: “There’s no American official c