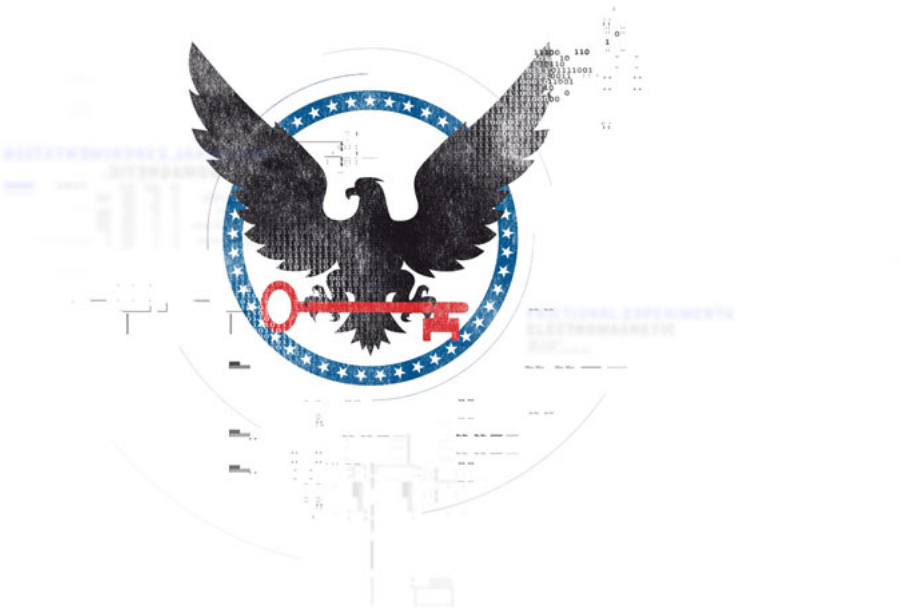
NSA Files
1The NSA Files2All the data about your data3A digital revolution4Are your details secure?5Who's watching6What now?Extended interviews
lNSA Files
1The NSA Files 2All the data about your data 3A digital revolution 4Are your details secure? 5Who's watching 6What now? Extended interviews

NSA FILES: DECODED

What the revelations mean for you.



Play
Current Time 0:00
/
Duration Time 0:00
Remaining Time -0:00
Loaded: 0%
Progress:
0%
00:00
Fullscreen
00:00
Mute

By EWEN MACASKILL and GABRIEL DANCE
Produced by FEILDING CAGE and GREG CHEN
Published on November 1, 2013

When Edward Snowden met journalists in his cramped room in Hong Kong's Mira hotel in June, his mission was ambitious. Amid the clutter of laundry, meal trays and his four laptops, he wanted to start a debate about mass surveillance.

He succeeded beyond anything the journalists or Snowden himself ever imagined. His disclosures about the NSA resonated with Americans from day one. But they also exploded round the world.

For some, like Congresswoman Zoe Lofgren, it is a vitally important issue, one of the biggest of our time: nothing less than the defence of democracy in the digital age.

stop auto-play
Zoe Lofgren
US congresswoman

But the intelligence agencies dismiss such claims, arguing that their programs are constitutional, and subject to rigorous congressional and judicial oversight. Secrecy, they say, is essential to meet their overriding aim of protecting the public from terrorist attacks.

stop auto-play
Stewart Baker
Former NSA general counsel

The debate has raged across time zones: from the US and Latin America to Europe and to Asia. Barack Obama cancelled a trip to Moscow in protest at Russian president Vladimir Putin's protection of Snowden. Brazilian president Dilma Rousseff cancelled a state visit to Washington in protest at the US spying on her. Bolivian president Evo Morales's plane was forced down in Vienna amid suspicion that Snowden was being smuggled out of Russia.

In Germany, a "livid" Angela Merkel accused the US of spying on her, igniting a furore that has seen the White House concede that new constraints on the NSA's activities may be necessary. Meanwhile, in Britain, prime minister David Cameron accused the Guardian of damaging national security by publishing the revelations, warning that if it did not "demonstrate some social responsibility it would be very difficult for government to stand back and not to act".

Caught in a net

by Nadja Popovich and Greg Chen

US internet companies, their co-operation with the NSA exposed by Snowden's documents, fear a worldwide consumer backlash, and claim they were forced into co-operation by the law.

DIANNE FEINSTEIN
Democratic US senator
KEITH ALEXANDER
Director of the NSA
BARACK OBAMA
US president
DAVID CAMERON
UK prime minister
DILMA ROUSSEFF
Brazilian president
LADAR LEVISON
Lavabit founder
RON WYDEN
Democratic US senator
JAMES CLAPPER
US director of national intelligence
EDWARD SNOWDEN
Computer analyst and whistleblower
ANGELA MERKEL
German chancellor
MARISSA MAYER
Yahoo CEO

Much of the NSA's defence is that the public should be unconcerned, summed up by the dictum: "If you have nothing to hide, you have nothing to fear." But civil liberties groups such as the Electronic Frontier Foundation and the American Civil Liberties Union warn that surveillance goes well beyond what Congress intended and what the US constitution allows.

stop auto-play
Chris Soghoian
Principal technologist, ACLU

Cell phones, laptops, Facebook, Skype, chat-rooms: all allow the NSA to build what it calls 'a pattern of life', a detailed profile of a target and anyone associated with them.

And the number of people caught up in this dragnet can be huge.

Three degrees of separation

by Kenton Powell and Greg Chen

You don't need to be talking to a terror suspect to have your communications data analysed by the NSA. The agency is allowed to travel "three hops" from its targets — who could be people who talk to people who talk to people who talk to you. Facebook, where the typical user has 190 friends, shows how three degrees of separation gets you to a network bigger than the population of Colorado. How many people are three "hops" from you?

Number of friends:

Login to Facebook
?
Connect to Facebook to get your friend count. Your information will not be saved.
LOGOUT

1ST DEGREE:
FRIENDS

2ND DEGREE:
FRIENDS OF FRIENDS

3RD DEGREE:
FRIENDS OF FRIENDS OF FRIENDS
Calculations are based on an analysis of Facebook that reports a typical user has an average of 190 friends and 14% of those friends are friends with each other.

Faced with growing public and political concern over the quantities of data it is collecting, the NSA has sought to reassure people, arguing that it collected only a tiny proportion of the world's internet traffic, roughly equivalent to a "dime on a basketball court". But in reality, that is still a huge amount of data. The Library of Congress, one of the biggest libraries in the world, gathers 5 terabytes a month. The NSA sucks up much, much more.

Since you began reading this, the NSA has selected
terabytes
of data for review. That's about
two-hour HD movies.

The NSA say it needs all this data to help prevent another terrorist attack like 9/11. In order to find the needle in the haystack, they argue, they need access to the whole haystack.

stop auto-play
Stewart Baker
Former NSA general counsel

Snowden recognises the value of the NSA in counter-terrorism, but thinks the spy agency has dangerously over-reached itself. He is a fugitive from US law, in exile in Russia. But the debate he wanted to start when he decided to become a whistleblower is now happening.

stop auto-play
Thomas Drake
Former senior executive, NSA
Part two

All the data about your data

One unseen consequence of the Snowden disclosures is the entry of the term 'metadata' into common usage. This is information about the time and location of a phone call or email, as opposed to the contents of those conversations or messages. The distinction forms the crux of the debate over the proper scope of NSA surveillance.

stop auto-play
Ron Wyden
US senator

The first Snowden document to be published by the Guardian was a secret court order showing that the NSA was collecting the telephone records of millions of US customers of Verizon, one of America's largest telecoms providers.

Verizon court order

Documents available in the desktop version of this interactive or at The NSA Files hub.

It is this program that has dominated US political debate since then. Early in October, Senator Dianne Feinstein, the chair of the Senate intelligence committee, wrote in USA Today: "The call-records program is not surveillance. It does not collect the content of any communication, nor do the records include names or locations. The NSA only collects the type of information found on a telephone bill: phone numbers of calls placed and received, the time of the calls and duration."

But privacy activists critical of the NSA surveillance program vehemently disagree, arguing not only that the collection is based on a legal interpretation that goes way beyond what Congress allowed, but also that metadata includes personal information, which can build a more detailed profile even than listening into content.

stop auto-play
Jameel Jaffer
Deputy legal director, ACLU

Your digital trail

by Feilding Cage

The chances are you are sharing a lot more personal information than you think …

Email
Facebook
Twitter
Camera
Google search
Web browsing
Phone calls

On metadata: what the experts say

Much of what the NSA does is of value to America and its friends round the world — even those it snoops on. The documents show the NSA providing vital information to American and allied forces in Afghanistan, defending the country against cyber attacks, snooping on Mexican drug cartels and helping break up worldwide criminal gangs involved in credit card theft.

Since the Snowden disclosures began, the NSA and the Obama administration have justified the agency's programs by claiming they have been crucial to 'successes' in counter-terrorism.

The NSA, in its defence, frequently argues that if today's surveillance programs existed before 9/11, it might have been able to stop those attacks. But this, too, is a matter of dispute. The intelligence agencies had a lot of capability before 9/11, and did pick up vital information, but failed to share it with one another or join up the dots.

Baker argues that the NSA has learned from its mistakes.

stop auto-play
Stewart Baker
Former NSA general counsel

But exactly how successful the bulk collection of US data has been in preventing terrorist attacks since 9/11 is a matter of dispute.

In the immediate wake of the early NSA revelations, the agency's director, General Keith Alexander, claimed the NSA surveillance had contributed to the prevention of 54 plots. But that number has been picked apart by the US media and Congress, forcing the NSA to revise it down. ProPublica have factchecked the 54 plots claim here and could only find evidence of four.

Eventually, deputy NSA director John Inglis conceded that, at most, one plot — which he has not specified — might have been disrupted by the bulk phone records program alone.

stop auto-play
Ron Wyden
US senator
Part three

A digital revolution

Two factors opened the way for the rapid expansion of surveillance over the past decade: the fear of terrorism created by the 9/11 attacks and the digital revolution that led to an explosion in cell phone and internet use.

But along with these technologies came an extension in the NSA's reach few in the early 1990s could have imagined. Details that in the past might have remained private were suddenly there for the taking.

stop auto-play
Chris Soghoian
Principal technologist, ACLU

NSA is helped by the fact that much of the world's communications traffic passes through the US or its close ally the UK – what the agencies refer to as "home-field advantage". The NSA has its own cable-intercept programs tapping traffic flowing into and across the US. These operate mainly under four codenames — BLARNEY, FAIRVIEW, OAKSTAR and STORMBREW — and are collectively known as Upstream collection.

The Snowden documents show that the NSA runs these surveillance programs through "partnerships" with major US telecom and internet companies. Some of these relationships go back decades, others are more recent, in the wake of 9/11 and with the growth of the internet.

The division inside the NSA that deals with collection programs that focus on private companies is Special Source Operations, described by Snowden as the "crown jewels" of the NSA.

In one top document, published here for the first time, SSO spelled out the importance of these commercial relationships which come under the heading "Corporate Partner Access".

In bald terms, it sets out its mission: "Leverage unique key corporate partnerships to gain access to high-capacity international fiber-optic cables, switches and/or routes throughout the world."

Tapping the cables

Documents available in the desktop version of this interactive or at The NSA Files hub.
stop auto-play
Jeremy Scahill
National security journalist

As well as fiber-optic cables in the US, the NSA has access to data gathered by close intelligence partners such as Britain's GCHQ.

The Snowden documents revealed the existence of Tempora, a program established in 2011 by GCHQ that gathers masses of phone and internet traffic by tapping into fiber-optic cables. GCHQ shares most of its information with the NSA.

Connected by cables

by Gabriel Dance

The United Kingdom is connected to 57 countries by fiber-optic cables. United States is connected to 63.

Connected
Not connected

—
Fiber-optic cable
.
Fiber-optic landing point
Distance between ocean surface and floor not drawn to scale
Source: TeleGeography

As well as its upstream collection programs, the NSA also has Prism, which, according to the Snowden documents, is the biggest single contributor to its intelligence reports. It is a "downstream" program – which means the agency collects the data from Google, Facebook, Apple, Yahoo and other US internet giants. One slide claims the agency has "direct access" to their servers, but this has been hotly disputed by the companies, who say they only comply with lawful requests for user data.

When the Guardian and the Washington Post revealed the existence of Prism the companies denied all knowledge of it and insisted that any co-operation with the intelligence agencies was compelled by law.

PRISM slides

Documents available in the desktop version of this interactive or at The NSA Files hub.

The names of many of the NSA's "corporate partners" are so sensitive that they are classified as "ECI" — Exceptionally Controlled Information — a higher classification level than the Snowden documents cover.

But some of the internet companies are named in the Special Source Operations briefing on Corporate Partner Access. A graphic comparing weekly reports involving the companies lists some of the Prism providers. Other companies on the list are protected by ECI covernames. Artifice, Lithium and Serenade are listed in other documents as covernames for SSO corporate partners, while Steelknight is described as an NSA partner facility.

This is the first time that data giving a sample of the number of intelligence records being generated per company has been published. It shows that over the period shown, June to July 2010, data from Yahoo generated by far the most NSA intelligence reports, followed by Microsoft, and then Google. All three companies are fighting through the courts to be allowed to release more detailed figures for the numbers of data requests they handle from US intelligence agencies.

Intelligence reports by company

Documents available in the desktop version of this interactive or at The NSA Files hub.
stop auto-play
Amie Stepanovich
Lawyer, Electronic Privacy Information Center

Not all companies have complied. Ladar Levison, the founder of Lavabit — a small, secure email provider used by Snowden — suspended operations in August rather than comply with a warrant that would have allowed the US government access to the data of all Lavabit's 400,000 customers.

stop auto-play
Ladar Levison
Founder of Lavabit

In a statement defending its surveillance programs, the NSA said: "What NSA does is collect the communications of targets of foreign intelligence value, irrespective of the provider that carries them. US service provider communications make use of the same information super highways as a variety of other commercial service providers. NSA must understand and take that into account in order to eliminate information that is not related to foreign intelligence.

"NSA works with a number of partners and allies in meeting its foreign-intelligence mission goals, and in every case those operations comply with US law and with the applicable laws under which those partners and allies operate."

But some members of Congress, such as Lofgren, who represents a Silicon Valley district, are unconvinced. She warns that the programs not only undermine individual privacy, but threaten the reputations of major American telecom and internet companies.

stop auto-play
Zoe Lofgren
US congresswoman
Part four

Are your details secure?

Millions of Americans struggling to get health insurance through Obamacare's new health exchanges are entering some of their most intimate details into computer systems.

The technology they rely on to keep that information secure — along with their emails, online shopping, banking and more — is encryption. But your data may not be as secure as you might hope.

Encrypting a message involves scrambling it through a combination of a randomly-generated key and mathematical jumbling. The NSA and its UK counterpart GCHQ regard this as the biggest threat to their ability to view the vast quantities of communications data they collect.

stop auto-play
Chris Soghoian
Principal technologist, ACLU

Internet companies have given assurances to their users about the security of communications. But the Snowden documents reveal that US and British intelligence agencies have successfully broken or circumvented much of online encryption.

Much of this, the documents reveal, was not done through traditional code-cracking, but instead by making deals with the industry to introduce weaknesses or backdoors into commercial encryption – and even working to covertly undermine the international standards on which encryption relies.

Computer security experts say that by doing this in their quest to access ever more data, the intelligence agencies have compromised the computers of hundreds of millions of ordinary internet users, and undermined one their other key priorities – protecting the US and UK from cyberattacks.

stop auto-play
Zoe Lofgren
US congresswoman

So is all encryption broken? Snowden, in a question-and-answer session on the Guardian website in June, said that much of the encryption is weak, so the NSA can frequently find ways round it, but there are strong crypto systems that can still be relied on. Given that Snowden was inside the system until May, he should know.

stop auto-play
Glenn Greenwald
Journalist

Pretty good privacy

by Greg Chen and Gabriel Dance

Snowden endorses a combination of Tor and PGP. Tor is a network that helps protect privacy and your physical location by providing anonymity, with volunteers bouncing communications round a network. PGP (Pretty Good Privacy) software can be used to encrypt data.

TOR

The TOR network is a protective layer that sits between the user and the internet. It provides an anonymous path between you and the sites you visit.
1. Your computer
The TOR program runs on your machine. It encrypts all information and sends it into the TOR network.
2. Into the network
Encrypted information, still considered unbreakable, is sent into the TOR network.
3. Untraceable
Your information travels through the TOR network taking random paths, making its origin and destination untraceable.
4. Decrypting the document
The exit node decrypts the untraceable information and sends it to its destination.
5. In the clear
From the exit node, unencrypted but anonymous data flows into and out of the internet.
6. The internet
Web sites see you as visiting from a random location, not identifiable to you.

PGP

Pretty **G**ood **P**rivacy is a data encryption technology commonly used for encrypting files, especially emails.
1. Sending the document
PGP depends on users having two keys: one public and one private. These two keys can only be used with one another.
2. Encrypting the document
The sender uses a random session key to encrypt the file. They sign the message with their private key, and encrypt the key using the receiver's public key.
3. An encrypted file
The file and the key are sent to the receiver. PGP, unlike TOR, does not anonymize the sender, but does provide strong encryption for the file.
4. Decrypting the document
The receiver verifies the signature with the sender's public key, and decrypts the key with their private key. They then decrypt the file using the key.
5. Message delivered
The receiver could then reciprocate the process using the sender's public and private keys.

Levison, the founder of secure email provider Lavabit, is facing a court case because he closed his company rather than hand over encryption keys.

stop auto-play
Ladar Levison
Founder of Lavabit
Part five

Who's watching

The publication of the Verizon phone records order had one immediate political impact. It revealed that at a Senate committee hearing in March 2013, the director of national intelligence, James Clapper, had given misleading testimony. He was asked by Senator Ron Wyden whether the NSA collected “any type of data at all on millions or hundreds of millions of Americans”. Clapper’s reply: “No, sir”.

Forced to revise his answer after the Guardian published the document in June, Clapper at first said that he had given “the least untruthful answer” possible in a public hearing. But then it emerged that Wyden’s office had given the DNI 24 hours notice of the question, and an opportunity to correct the record shortly thereafter. Clapper changed his account to say that he had simply forgotten about collection of domestic phone records.

The erroneous testimony sparked calls for Clapper’s dismissal and has become a glaring example of failings in the oversight arrangements that are supposed to govern NSA surveillance programs.

stop auto-play
Jeremy Scahill
National security journalist

The Snowden disclosures have led many on Capitol Hill and beyond to conclude that the political and legal mechanisms necessary to hold the NSA accountable in functioning democracy are no longer fit for purpose.

The Foreign Intelligence Surveillance Act of 1978 (Fisa) was intended to curtail the NSA’s ability to use its capabilities against Americans. It was passed as part of a backlash against one of the biggest controversies of that era: the unlawful surveillance by the intelligence agencies of US political activists, trade union leaders and civil

rights leaders.

Fisa codified in law for the first time that the NSA was about foreign intelligence. If there was a suspicion about a spy or some agent of a foreign power operating in the US, the NSA and the FBI could apply for a warrant in a new surveillance court, the Fisa court.

But since then, according to Wyden, the way the laws work in practice by the intelligence agencies has become shrouded in secrecy.

The 2008 Fisa Amendments Act, renewed in 2012, allows for the collection of communications without a warrant, where at least one end of the communications is a non-US person.
stop auto-play
Ron Wyden
US senator

The NSA legal basis — disputed — for bulk collection of Americans' phone data comes under a different law, section 215 of the 2001 Patriot Act. The Bush administration, in secret after 9/11, turned loose the NSA to collect bulk email records domestically.The NSA interpreted section 215 of the Patriot Act as allowing them to collect phone metadata in the US.

The legal case

by Kenton Powell

The NSA asserts that a number of laws and legal precedents justify its surveillance programs. These are a few of those key laws and precedents:What legal authorities does the NSA rely on to justify the collection of:

phone records of an American in the US?

Foreign Intelligence Surveillance Act (Fisa) of 1978

Foreign Intelligence Surveillance Act (Fisa) of 1978
Fisa provides the foundation for foreign intelligence surveillance. The Act establishes procedures for the collection of this intelligence, and a secret court to oversee those activities. Fisa has been amended since to allow for increased warrantless surveillance.

Executive Order 12333

Executive Order 12333
Signed in 1981 by President Reagan, and most recently amended by President Bush in 2004, this order broadly authorizes the collection of all information for the purpose of "national defense" not prohibited by other applicable laws.

Patriot Act of 2001: Sections 214, 216

Patriot Act of 2001: Sections 214, 216
Amends FISA allowing the collection of certain wire or electronic communication metadata to communications relevant to a terrorist or espionage investigation instead of communications likely to be those of a terrorist or spy.

Patriot Act of 2001: Section 215

Patriot Act of 2001: Section 215
Amends FISA, allowing the government to order the collection of "tangible things" that aid in an terrorism or espionage investigation. These "things" don't need to pertain directly to a target but instead only be relevant to an investigation.

Fisa Amendments Act of 2008: Section 702

Fisa Amendments Act of 2008: Section 702
Amends Fisa and requires the establishment of procedures for targeting non-US persons overseas. The government may not intentionally target a US person but the NSA has revealed that it does unintentionally collect American communications.

Fisa Amendments Act of 2008: Sections 703, 704

Fisa Amendments Act of 2008: Sections 703, 704
Amends FISA and establishes procedures for targeting US persons overseas. In these cases, surveillance of a US person can be authorized without a warrant because the US person is outside the country.

National Security Letter

National Security Letter
National security letters are administrative subpoenas that allow the FBI to compel the recipient to divulge subscriber and billing information relevant to a national security investigation. These letters require no judicial review and the recipient is prohibited from revealing the contents or existence of the letter.

Fisa Court Order

Fisa court Order
These orders are issued to compel entities to furnish information the government has requested. The court operates in secrecy and is not subject to public oversight.
Source: Electronic Privacy Information Center

The Fisa court and its proceedings are secret, or at least they were until the Snowden revelations. Given this, it is nearly impossible to challenge its interpretation of the law. The government is the only petitioner before the court, with no advocates for privacy interests. The NSA argues that since that it is engaged in covert operations, it is hardly surprising that the court proceedings are secret.

stop auto-play
Amie Stepanovich
Lawyer, Electronic Privacy Information Center

In January 2009, the FISA court was notified that the NSA had been querying business records metadata "in a manner that appear[ed] to the Court to be directly contrary" to the court's order allowing it to so. In response, the FISA court ordered the government to explain itself. These documents detail this exchange as the NSA struggled to understand the business records program and ensure compliance.

An unhappy court

by Kenton Powell
To see this interactive, please visit in with a desktop browser.
Fisa court discovers unauthorized querying and demands answers

Document
Order Regarding Preliminary Notice of Compliance Incident Dated January 15, 2009
January 28, 2009
Reggie Walton, FISC
Summary
On January 28 2009, the government is ordered to respond to a series of questions related to the unauthorized querying of telephone records through the use of an "alert list", which included numbers not reviewed for querying. In this order, Judge Walton states the responses to the court's questions will determine whether the modification or rescission of the order authorizing the collection of querying and/or other remedial measures are required.
Key Quote
The court is exceptionally concerned about what appears to be a flagrant violation of its order in this matter and, while the court will not direct that specific officials of the executive branch provide sworn declarations in response to this order, the court expects that the declarants will be officials of sufficient stature that they have the authority to speak on behalf of the executive branch.
—Reggie Walton
DoJ and NSA respond to court

Document
Memorandum of the United States in Response to the Court's Order Dated January 28, 2009
February 17, 2009
Matthew Olsen, DoJ and
Keith Alexander, NSA
Summary
In response, the government acknowledges the NSA's "alert list" process was inaccurately described to the court and the order did not provide the "authority to employ the list in the manner in which it did." The government asks the court not to rescind or modify the order allowing the collection and querying of metadata and details remedial action it's begun to undertake in its collection of metadata including an "end-to-end system engineering and process reviews."
Key Quote
In its reports to the court, NSA stated the alert list only contained telephone identifiers that satisfied the [reasonable articulable standard]. In reality, the majority of identifiers on the alert list were [counterterrorism] identifiers that had not been assessed for [reasonable articulable standard].
—Keith Alexander
NSA reports more incidents of unauthorized use of data

Document
Notice of Compliance Incidents
February 26, 2009
Redacted and
Keith Alexander, NSA
Summary
In response to the January 28 2009 order, the director of the NSA ordered an audit of all queries made of the [business records] metadata since 2008 to determine if any of the queries during that period were made using telephone identifiers for which NSA had not determined that a reasonable, articulable suspicion existed as required by the

court. One tool and three analysts had queried the records with telephone identifiers not approved for querying.

Key Quote

During an end-to-end review of the NSA's technical infrastructure that I ordered in response to the compliance incident that the DoJ reported to the court on 15 January 2009, NSA personnel determined on 18 February 2009 that an NSA analytics tool known as [redacted] was querying both EO 12333 and the Business Records data and that such queries would not have been limited to [reasonable articulable standard] approved telephone identifiers.

—Keith Alexander

Court orders NSA to continue to collect metadata but not use it

Document

Order

March 2, 2009

Reggie Walton, FISC

Summary

After an order allowing the collection of metadata expires, Judge Walton permits the NSA to continue to collect telephone metadata but prohibits the government from accessing the metadata for the purposes of obtaining foreign intelligence and requires the NSA to submit various documentation following the completion of its end-to-end review.

Key Quote

The government may request through a motion that the court authorize querying of the [business records] metadata for purposes of obtaining foreign intelligence on a case-by-case basis.

—Reggie Walton

Court orders NSA to submit a list of those outside of the NSA with access to data

Document

Order

June 22, 2009

Reggie Walton, FISC

Summary

Following disclosure to the court that the NSA was sharing query results outside the NSA, Judge Walton orders the NSA to submit a report every week with every instance in the prior week that metadata collections were shared with anyone outside the NSA.

Key Quote

With regard to [redacted] BR 09-06, the government shall, by 5.00pm each Friday, commencing on July 3, 2009, file with the court a report listing each instance during the seven-day period ending the previous Friday in which NSA has shared, in any form, information obtained or derived from the [redacted] [business records] metadata collections with anyone outside NSA.

—Reggie Walton

NSA completes formal end-to-end review

Document

Notice of Compliance Incidents

June 25, 2009

NSA

Summary

The NSA finishes a "systems engineering and process review".

Key Quote

The problems NSA experienced stemmed from a basic lack of shared understanding among the key mission, technology, legal and oversight stakeholders of the full scope of the program to include its implementation and end-to-end design.

Government submits reports and testimony to court detailing review and reforms summary

Document

Report of the United States

August 17, 2009

David Kris, DoJ

Keith Alexander, NSA

Robert Mueller, FBI

Summary

This report describes compliance issues identified by NSA during its end-to-end review of the metadata collection program. The report also includes a discussion of the value of the program by the FBI and NSA directors.

Key Quote

The court entrusted NSA with extraordinary authority, and with it came the highest responsibility for compliance and protection of privacy rights. In several instances, NSA implemented its authority in a manner inconsistent with the orders, and some of these inconsistencies were not recognized for more than two and a half years.

—Keith Alexander
Court allows NSA to continue to collect and query data

Document
Primary Order
September 3, 2009
Reggie Walton, FISC
Summary
After the government's August 19 report, the court reauthorizes the metadata collection program and removes additional Fisa court oversight measures.
Key Quote
Subject to restriction and procedures below, the [business records] metadata may be accessed for purposes of obtaining foreign intelligence information through contact chaining [redacted] ("queries") using telephone identifiers…
—Reggie Walton
Source: Electronic Privacy Information Center
stop auto-play
Stewart Baker
Former NSA general counsel

In spite of Baker's contention, the court has approved almost all government surveillance requests over the last 35 years.

Judges of the Fisa court

by Kenan Davis

The Fisa court reviews applications made by the executive branch for electronic surveillance in cases related to national security. The judges are appointed by the chief justice of the US supreme court. Since the Fisa court's formation in 1978, there have been three chief justices, all appointed by Republican presidents. Throughout the court's existence, the demographics of the judges serving on the court have been largely homogeneous. Sixty-four percent have been white men appointed to their federal bench by Republican presidents, while only 4% were non-white, Democratic appointees.

- Current Court Members

- Republican Appointees
- Democratic Appointees

- Male
- Female

- White
- Hispanic
- African American

out of 72 judges appointed to the court
The USA Patriot Act of 2001 increased the Fisa court from seven to eleven members. The eleven judges must come from at least seven judicial circuits, and at least three must live within twenty miles of the District of Columbia.
Sources: Federation of American Scientists, Federal Judicial Center

The NSA is also subject to congressional oversight. But the limitations of this have become clearer over the past few months, with many members of Congress directly contradicting Obama's persistent claim that they have signed off these programs, and insisting they had been totally unaware of the scope of the agency's activities.

stop auto-play
Zoe Lofgren
US congresswoman

The politicians tasked with the greatest scrutiny are the Senate and House intelligence committees. Most of these — in particular Feinstein, the Senate intelligence committee chairwoman — have tended to be staunch defenders of the NSA.

The long-term sceptics, such as Wyden and his Senate colleague Udall, have been a lonely band. Even now, they believe they face an uphill struggle to achieve meaningful reform of the NSA.

stop auto-play
Ron Wyden
US senator
Part six

What now?

The debate Snowden wanted is happening. That in itself is a major achievement.

stop auto-play
Stewart Baker
Former NSA general counsel

But debate has expanded well beyond the confines of Capitol Hill, touching on individuals and groups throughout the US and elsewhere in the world.

One group feeling the immediate impact is journalists and their sources. The Snowden revelations have sent a chill through those reporters covering national security issues. If the NSA can easily gather details about who a reporter phoned or emailed, that sends a signal to whistleblowers that their anonymity can no longer be protected.

stop auto-play
Jameel Jaffer
Deputy legal director, ACLU

Public opinion is polarized over surveillance, but polls show a jump in concern over privacy in the wake of Snowden's revelations. A Pew poll at the end of July found that for the first time in a decade, the majority of Americans are more concerned about the government infringing on their civil liberties than about a potential terrorist attack.

The shift is reflected in the change in attitudes over the past two years on a series of privacy issues.

Shifting sentiment?

by Kenan Davis and Kenton Powell

According to a recent study, the majority of Americans believe that preserving the rights of US citizens is more important than preventing terrorist attacks. Since the NSA revelations, Americans have become more opposed to government surveillance that infringes on civil liberties.

Source: The Associated Press-NORC Center for Public Affairs Research

In the end, it may be through the courts rather than Congress that genuine reform may come. Privacy groups such as the Electronic Privacy Information Center and the Electronic Frontier Foundation launched lawsuits that have led to disclosure of hundreds of pages of Fisa rulings on Section 215. GCHQ and NSA surveillance is facing a legal challenge at the European court of human rights from Big Brother Watch, English PEN and Open Rights Group.

Silicon Valley is also taking action through the courts. Google, Microsoft and Yahoo, facing a backlash from their users in the US and overseas over mass surveillance, are fighting to be allowed to be more transparent about their dealings with the intelligence agencies. These companies, along with Facebook, Apple and AOL have also written to the Senate intelligence committee demanding reform.

The political fallout from the NSA revelations began slowly, but in July it became dramatically apparent in Congress. The occasion was a vote in the House on Republican Justin Amash's amendment to curtail funding for the NSA's bulk collection of phone records for millions of Americans.

stop auto-play
Glenn Greenwald
Journalist

The amendment only narrowly failed to get through, with 205 in favour and 217 against. Support for change brought conservatives and liberals together in an unusual alliance.

A bipartisan Congress

by Kenan Davis

Congress during the Obama administration has been marked by members voting time and again along fiercely partisan lines. Bipartisanship has become increasingly rare. On legislation concerning the budget, healthcare, abortion and domestic abuse, members were less likely to vote against their party. The vote in July was one of the the rarities, splitting ranks within both parties. Analysis by the Guardian reveals that it was one of the least partisan votes — beaten only by food aid reform and flood protection — in a Congress defined by hardline partisanship.

- Republican majority
- Republican minority
- Democratic minority
- Democratic majority

Vote to Limit NSA Data Collection

3rd most cross-partisan of 568 votes
With both parties deeply divided, unusual coalitions were formed with centrist Republican and Democrats uniting against liberal Democrats and libertarian Republicans. The split exposed each party's inability to find consensus on the government's controversial practice of gathering private data.

Vote to Approve a Three-Month Debt Limit Extension

46th of 568 votes
The majority of Republicans supported a plan to increase the debt limit for a short period while stipulating that members of Congress would receive delayed pay if they didn't pass a budget resolution. Democratic skepticism of the temporary reprieve resulted in a split vote.

Vote to Renew the Violence Against Women Act

98th of 568 votes
The Democrats unanimously supported the reauthorization of the Violence Against Women Act, while the Republicans were divided over the law's renewal, which included protections for gay, bisexual, and transgender victims of domestic abuse.

Vote to Repeal the Affordable Care Act

417th of 568 votes

Republicans and Democrats united against each other and took opposing sides on a bill sponsored by Republican Congresswoman Michele Bachmann.
Figures are in percentages
Source: Clerk's Office of the U.S. House of Representatives
Notes: Quorum call, Speaker election and present votes have been excluded. Votes have been sorted by the average of each party's majority in a vote. Includes votes up to October 30, 2013.

There are now several major pieces of legislation going through Congress that would introduce at least some reform of the NSA. Among those, the one backed by Feinstein and passed by her committee is the least radical, offering proposals for greater transparency but basically maintaining the status quo. The bulk collection of Americans' phone call data would be enshrined in US law.

More far-reaching is the proposed Intelligence Oversight and Reform Act, with bipartisan support from senators Wyden, Udall, Richard Blumenthal and Rand Paul. It would ban the collection of internet communication data; close loopholes that allow snooping on Americans without a warrant; reform the Fisa court; and provide some protection for companies faced with handing over data to the NSA.

Another bipartisan bill, backed by high-ranking senator Patrick Leahy and congressman Jim Sensenbrenner, who was one of the architects of the Patriot Act, would also end bulk collection of phone records. As part of reform of the Fisa court, it is proposed that a special advocate be created.

stop auto-play
Ron Wyden
US senator

The Guardian has published a selection of classified NSA documents, passed on by whistleblower Edward Snowden. Some have been redacted to preserve author anonymity. Explore the NSA documents in full below.

Explore the documents

Documents available in the desktop version of this interactive or at The NSA Files hub.

Extended interviews

What the experts say:

What the experts say

Select an expert
Select a topic

Video: Bob Sacha
Production: Kenan Davis, Nadja Popovich, Kenton Powell, Ewen MacAskill, Ruth Spencer, Lisa van Gelder
Additional Production: Spencer Ackerman, Kayla Epstein, Paul Lewis, Amanda Michel, Katie Rogers, Dominic Rushe
close
hello world
here is some text