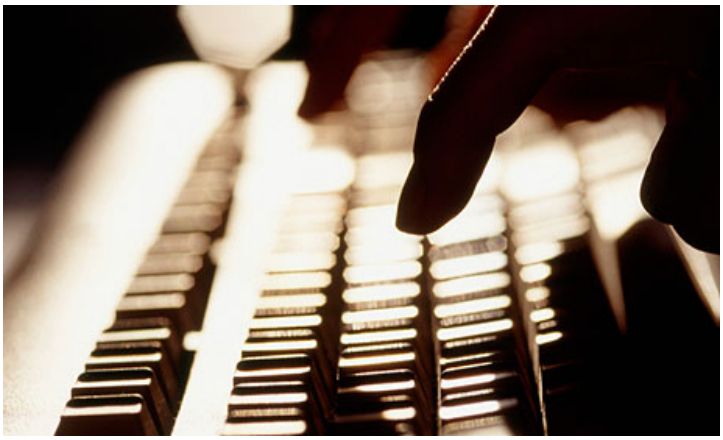
The top secret rules that allow NSA to use US data without a warrant

Fisa court submissions show broad scope of procedures governing NSA's surveillance of Americans' communication

• Document one: procedures used by NSA to target non-US persons
• Document two: procedures used by NSA to minimise data collected from US persons

Glenn Greenwald and **James Ball**
theguardian.com, Thursday 20 June 2013 23.59 BST

Jump to comments (…)



The documents show that discretion as to who is actually targeted lies directly with the NSA's analysts. Photograph: Martin Rogers/Workbook Stock/Getty

Top secret documents submitted to the court that oversees surveillance by US intelligence agencies show the judges have signed off on broad orders which allow the NSA to make use of information "inadvertently" collected from domestic US communications without a warrant.

The Guardian is publishing in full two documents submitted to the secret Foreign Intelligence Surveillance Court (known as the Fisa court), signed by Attorney General Eric Holder and stamped 29 July 2009. They detail the procedures the NSA is required to follow to target "non-US persons" under its foreign intelligence powers and what the agency does to minimize data collected on US citizens and residents in the course of that surveillance.

The documents show that even under authorities governing the collection of foreign intelligence from foreign targets, US communications can still be collected, retained and used.

Article history

The NSA Files: Decoded

What the surveillance revelations mean for you

World news
The NSA files · NSA · Obama administration · Prism · Privacy · Surveillance · US national security

Law
Fisa court · US constitution and civil liberties

Series
Glenn Greenwald on security and liberty

More from Glenn Greenwald on security and liberty on

World news
The NSA files · NSA · Obama administration · Prism · Privacy · Surveillance · US national security

The procedures cover only part of the NSA's surveillance of domestic US communications. The bulk collection of domestic call records, as first revealed by the Guardian earlier this month, takes place under rolling court orders issued on the basis of a legal interpretation of a different authority, section 215 of the Patriot Act.

The Fisa court's oversight role has been referenced many times by Barack Obama and senior intelligence officials as they have sought to reassure the public about surveillance, but the procedures approved by the court have never before been publicly disclosed.

The top secret documents published today detail the circumstances in which data collected on US persons under the foreign intelligence authority must be destroyed, extensive steps analysts must take to try to check targets are outside the US, and reveals how US call records are used to help remove US citizens and residents from data collection.

However, alongside those provisions, the Fisa court-approved policies allow the NSA to:

• Keep data that could potentially contain details of US persons for up to five years;

• Retain and make use of "inadvertently acquired" domestic communications if they contain usable intelligence, information on criminal activity, threat of harm to people or property, are encrypted, or are believed to contain any information relevant to cybersecurity;

• Preserve "foreign intelligence information" contained within attorney-client communications;

• Access the content of communications gathered from "U.S. based machine[s]" or phone numbers in order to establish if targets are located in the US, for the purposes of ceasing further surveillance.

The broad scope of the court orders, and the nature of the procedures set out in the documents, appear to clash with assurances from President Obama and senior intelligence officials that the NSA could not access Americans' call or email information without warrants.

The documents also show that discretion as to who is actually targeted under the NSA's foreign surveillance powers lies directly with its own analysts, without recourse to courts or superiors – though a percentage of targeting decisions are reviewed by internal audit teams on a regular basis.

Since the Guardian first revealed the extent of the NSA's collection of US communications, there have been repeated calls for the legal basis of the programs to be released. On Thursday, two US congressmen introduced a bill compelling the Obama administration to declassify the secret legal justifications for NSA surveillance.

The disclosure bill, sponsored by Adam Schiff, a California Democrat, and Todd Rokita, an Indiana Republican, is a complement to one proposed in the Senate last week. It would "increase the transparency of the Fisa Court and the state of the law in this area," Schiff told the Guardian. "It would give the public a better understanding of the safeguards, as well as the scope of these programs."

Section 702 of the Fisa Amendments Act (FAA), which was renewed for five years last December, is the authority under which the NSA is allowed to collect large-scale data, including foreign communications and also communications between the US and other countries, provided the target is overseas.

FAA warrants are issued by the Fisa court for up to 12 months at a time, and authorise the collection of bulk information – some of which can include communications of US citizens, or people inside the US. To intentionally target either of those groups requires an individual warrant.

One-paragraph order

One such warrant seen by the Guardian shows that they do not contain

Law
Fisa court · US constitution and civil liberties

More on this story

Glenn Greenwald: Fisa court oversight: a look inside a secret and empty process
Glenn Greenwald: Obama and other NSA defenders insist there are robust limitations on surveillance but the documents show otherwise

NSA surveillance: don't underestimate the extraordinary power of metadata

Procedures used by NSA to target non-US persons: Exhibit A – full document

Procedures used by NSA to minimize data collection from US persons: Exhibit B – full document

Fisa court warrant authorising NSA surveillance procedures – full document

Live: Follow NSA-related developments as controversy over leaks continues to make headlines

detailed legal rulings or explanation. Instead, the one-paragraph order, signed by a Fisa court judge in 2010, declares that the procedures submitted by the attorney general on behalf of the NSA are consistent with US law and the fourth amendment.

Those procedures state that the "NSA determines whether a person is a non-United States person reasonably believed to be outside the United States in light of the totality of the circumstances based on the information available with respect to that person, including information concerning the communications facility or facilities used by that person".

It includes information that the NSA analyst uses to make this determination – including IP addresses, statements made by the potential target, and other information in the NSA databases, which can include public information and data collected by other agencies.

Where the NSA has no specific information on a person's location, analysts are free to presume they are overseas, the document continues.

"In the absence of specific information regarding whether a target is a United States person," it states "a person reasonably believed to be located outside the United States or whose location is not known will be presumed to be a non-United States person unless such person can be positively identified as a United States person."

If it later appears that a target is in fact located in the US, analysts are permitted to look at the content of messages, or listen to phone calls, to establish if this is indeed the case.

Referring to steps taken to prevent intentional collection of telephone content of those inside the US, the document states: "NSA analysts may analyze content for indications that a foreign target has entered or intends to enter the United States. Such content analysis will be conducted according to analytic and intelligence requirements and priorities."

Details set out in the "minimization procedures", regularly referred to in House and Senate hearings, as well as public statements in recent weeks, also raise questions as to the extent of monitoring of US citizens and residents.

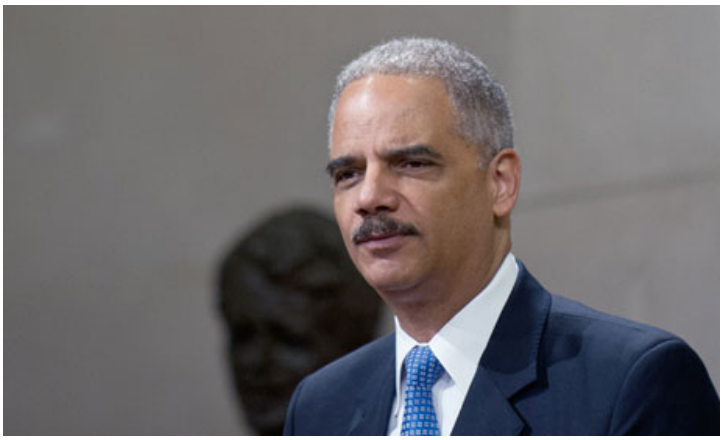
NSA minimization procedures signed by Holder in 2009 set out that once a target is confirmed to be within the US, interception must stop immediately. However, these circumstances do not apply to large-scale data where the NSA claims it is unable to filter US communications from non-US ones.

The NSA is empowered to retain data for up to five years and the policy states "communications which may be retained include electronic communications acquired because of limitations on the NSA's ability to filter communications".

Even if upon examination a communication is found to be domestic – entirely within the US – the NSA can appeal to its director to keep what it has found if it contains "significant foreign intelligence information", "evidence of a crime", "technical data base information" (such as encrypted communications), or "information pertaining to a threat of serious harm to life or property".

Domestic communications containing none of the above must be destroyed. Communications in which one party was outside the US, but the other is a US-person, are permitted for retention under FAA rules.

The minimization procedure adds that these can be disseminated to other agencies or friendly governments if the US person is anonymised, or including the US person's identity under certain criteria.



Holder's 'minimization procedure' says once a target is confirmed to be in the US, interception of communication must stop. Photo: Nicholas Kamm/AFP/Getty Images

A separate section of the same document notes that as soon as any intercepted communications are determined to have been between someone under US criminal indictment and their attorney, surveillance must stop. However, the material collected can be retained, if it is useful, though in a segregated database:

"The relevant portion of the communication containing that conversation will be segregated and the National Security Division of the Department of Justice will be notified so that appropriate procedures may be established to protect such communications from review or use in any criminal prosecution, while preserving foreign intelligence information contained therein," the document states.

In practice, much of the decision-making appears to lie with NSA analysts, rather than the Fisa court or senior officials.

A transcript of a 2008 briefing on FAA from the NSA's general counsel sets out how much discretion NSA analysts possess when it comes to the specifics of targeting, and making decisions on who they believe is a non-US person. Referring to a situation where there has been a suggestion a target is within the US.

"Once again, the standard here is a reasonable belief that your target is outside the United States. What does that mean when you get information that might lead you to believe the contrary? It means you can't ignore it. You can't turn a blind eye to somebody saying: 'Hey, I think so and so is in the United States.' You can't ignore that. Does it mean you have to completely turn off collection the minute you hear that? No, it means you have to do some sort of investigation: 'Is that guy right? Is my target here?" he says.

"But, if everything else you have says 'no' (he talked yesterday, I saw him on TV yesterday, even, depending on the target, he was in Baghdad) you can still continue targeting but you have to keep that in mind. You can't put it aside. You have to investigate it and, once again, with that new information in mind, what is your reasonable belief about your target's location?"

The broad nature of the court's oversight role, and the discretion given to NSA analysts, sheds light on responses from the administration and internet companies to the Guardian's disclosure of the PRISM program. They have stated that the content of online communications is turned over to the NSA only pursuant to a court order. But except when a US citizen is specifically targeted, the court orders used by the NSA to obtain that information as part of Prism are these general FAA orders, not individualized warrants specific to any individual.

Once armed with these general orders, the NSA is empowered to compel telephone and internet companies to turn over to it the communications of any individual identified by the NSA. The Fisa court plays no role in the selection of those individuals, nor does it monitor who is selected by the NSA.

The NSA's ability to collect and retain the communications of people in

the US, even without a warrant, has fuelled congressional demands for an estimate of how many Americans have been caught up in surveillance.

Two US senators, Ron Wyden and Mark Udall – both members of the Senate intelligence committee – have been seeking this information since 2011, but senior White House and intelligence officials have repeatedly insisted that the agency is unable to gather such statistics.

Comments

More from Glenn Greenwald on security and liberty

A critical, campaigning column on vital issues of civil rights, freedom of information and justice – and their enemies, from the award-winning journalist, former constitutional litigator and author of three New York Times bestsellers.

Follow @ggreenwald on Twitter or email him at glenn.greenwald@guardiannews.com

Latest:
31 Oct 2013: On leaving the Guardian | Glenn Greenwald

Next:
22 Jun 2013: On the Espionage Act charges against Edward Snowden | Glenn Greenwald

Previous:
19 Jun 2013: Fisa court oversight: a look inside a secret and empty process | Glenn Greenwald

Glenn Greenwald on security and liberty index