

*Wikimedia Foundation v. NSA*  
No. 15-cv-0062-TSE (D. Md.)

# Plaintiff's Exhibit 27

# The Guardian



## XKeyscore: NSA tool collects 'nearly everything a user does on the internet'

**. XKeyscore gives 'widest-reaching' collection of online data . NSA analysts require no prior authorization for searches . Sweeps up emails, social media activity and browsing history . NSA's XKeyscore program - read one of the presentations**

**Glenn Greenwald**

Wed 31 Jul 2013 08.56 EDT

A top secret National Security Agency program allows analysts to search with no prior authorization through vast databases containing emails, online chats and the browsing histories of millions of individuals, according to documents provided by whistleblower Edward Snowden.

The NSA boasts in training materials that the program, called XKeyscore, is its "widest-reaching" system for developing intelligence from the internet.

The latest revelations will add to the intense public and congressional debate around the extent of NSA surveillance programs. They come as senior intelligence officials testify to the Senate judiciary committee on Wednesday, releasing classified documents in response to the Guardian's earlier stories on bulk collection of phone records and Fisa surveillance court oversight.

The files shed light on one of Snowden's most controversial statements, made in his first video interview published by the Guardian on June 10.

"I, sitting at my desk," said Snowden, could "wiretap anyone, from you or your accountant, to a federal judge or even the president, if I had a personal email".

US officials vehemently denied this specific claim. Mike Rogers, the Republican chairman of the House intelligence committee, said of Snowden's assertion: "He's lying. It's impossible for him to do what he was saying he could do."

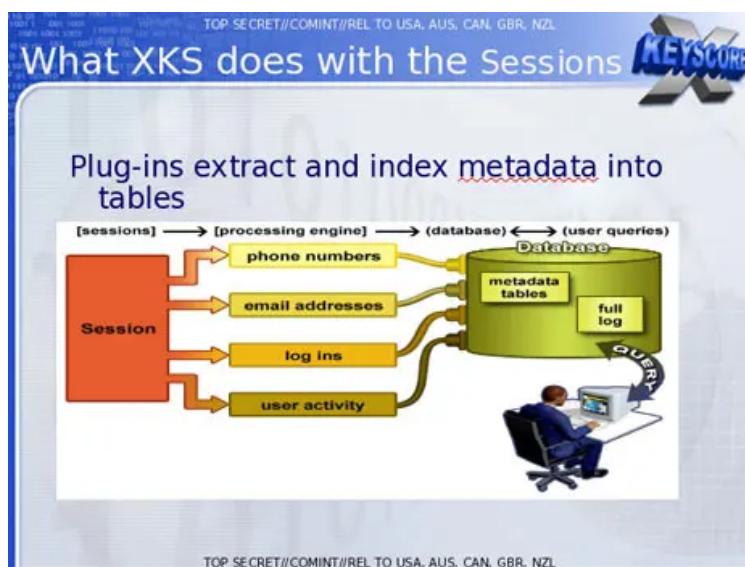
But training materials for XKeyscore detail how analysts can use it and other systems to mine enormous agency databases by filling in a simple on-screen form giving only a broad justification for the search. The request is not reviewed by a court or any NSA personnel before it is processed.

XKeyscore, the documents boast, is the NSA's "widest reaching" system developing intelligence from computer networks - what the agency calls Digital Network Intelligence (DNI). One presentation claims the program covers "nearly everything a typical user does on the internet", including the content of emails, websites visited and searches, as well as their metadata.

Analysts can also use XKeyscore and other NSA systems to obtain ongoing "real-time" interception of an individual's internet activity.

Under US law, the NSA is required to obtain an individualized Fisa warrant only if the target of their surveillance is a 'US person', though no such warrant is required for intercepting the communications of Americans with foreign targets. But XKeyscore provides the technological capability, if not the legal authority, to target even US persons for extensive electronic surveillance without a warrant provided that some identifying information, such as their email or IP address, is known to the analyst.

One training slide illustrates the digital activity constantly being collected by XKeyscore and the analyst's ability to query the databases at any time.



KS1 Photograph: Guardian

The purpose of XKeyscore is to allow analysts to search the metadata as well as the content of emails and other internet activity, such as browser history, even when there is no known email

Case 1:15-cv-00662-TSE Document 168-31 Filed 12/18/18 Page 4 of 11  
 account (a "selector" in NSA parlance) associated with the individual being targeted.

Analysts can also search by name, telephone number, IP address, keywords, the language in which the internet activity was conducted or the type of browser used.

One document notes that this is because "strong selection [search by email address] itself gives us only a very limited capability" because "a large amount of time spent on the web is performing actions that are anonymous."

The NSA documents assert that by 2008, 300 terrorists had been captured using intelligence from XKeyscore.

Analysts are warned that searching the full database for content will yield too many results to sift through. Instead they are advised to use the metadata also stored in the databases to narrow down what to review.

A slide entitled "plug-ins" in a December 2012 document describes the various fields of information that can be searched. It includes "every email address seen in a session by both username and domain", "every phone number seen in a session (eg address book entries or signature block)" and user activity - "the webmail and chat activity to include username, buddylist, machine specific cookies etc".

## Email monitoring

In a second Guardian interview in June, Snowden elaborated on his statement about being able to read any individual's email if he had their email address. He said the claim was based in part on the email search capabilities of XKeyscore, which Snowden says he was authorized to use while working as a Booz Allen contractor for the NSA.

One top-secret document describes how the program "searches within bodies of emails, webpages and documents", including the "To, From, CC, BCC lines" and the 'Contact Us' pages on websites".

To search for emails, an analyst using XKS enters the individual's email address into a simple online search form, along with the "justification" for the search and the time period for which the emails are sought.

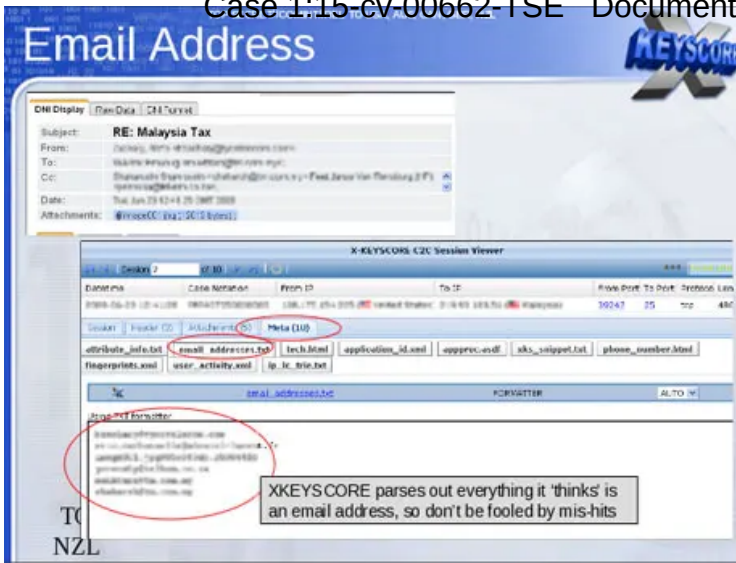
The screenshot shows a web browser window titled "The unofficial Xkeyscore Users Guide". Below the title bar, there is a search bar with "7" entered and a "Fit Page Width" button. The main content area is titled "Email Addresses Query:" and contains the following text: "One of the most common queries is (you guessed it) an **Email Address Query** searching for an email address. To create a query for a specific email address, you have to fill in the name of the query, justify it and set a date range then you simply fill in the email address(es) you want to search on and submit."

Below this text, it says "That would look something like this..." and shows a form titled "Search: Email Addresses". The form has the following fields:
 

- Query Name:
- Justification:
- Additional Justification:
- Miranda Number:
- Date Range:  Start:
- Email Username:
- @Domain:

 At the top of the form, there are links for "Fields", "Advanced Features", "Show Hidden Search Fields", "Clear Search Values", and "Reload Last Search Values".

KS2 Photograph: Guardian

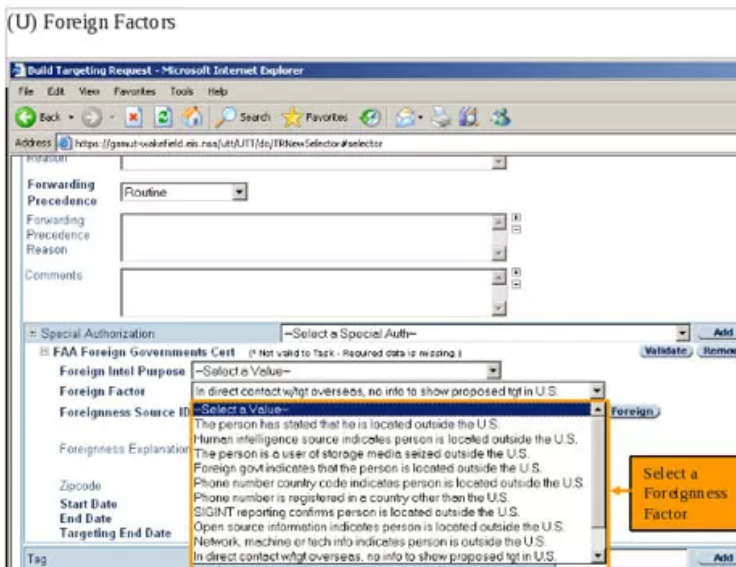


KS3edit2 Photograph: Guardian

The analyst then selects which of those returned emails they want to read by opening them in NSA reading software.

The system is similar to the way in which NSA analysts generally can intercept the communications of anyone they select, including, as one NSA document put it, "communications that transit the United States and communications that terminate in the United States".

One document, a top secret 2010 guide describing the training received by NSA analysts for general surveillance under the Fisa Amendments Act of 2008, explains that analysts can begin surveillance on anyone by clicking a few simple pull-down menus designed to provide both legal and targeting justifications. Once options on the pull-down menus are selected, their target is marked for electronic surveillance and the analyst is able to review the content of their communications:

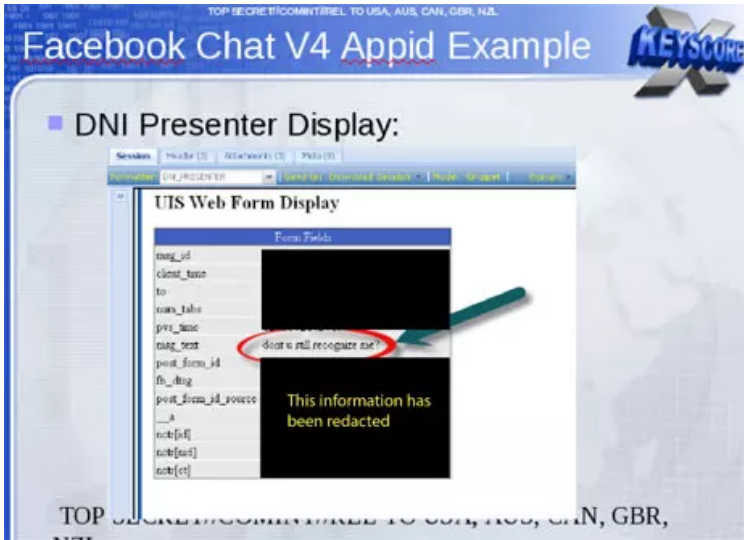


KS4 Photograph: Guardian

### Chats, browsing history and other internet activity

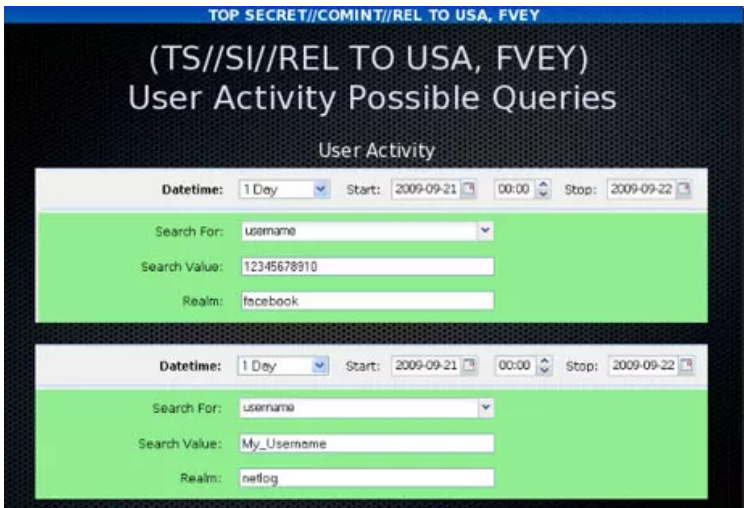
Beyond emails, the XKeyscore system allows analysts to monitor a virtually unlimited array of other internet activities, including those within social media.

An NSA tool called DNI Presenter, used to read the content of stored emails, also enables an analyst using XKeyscore to read the content of Facebook chats or private messages.



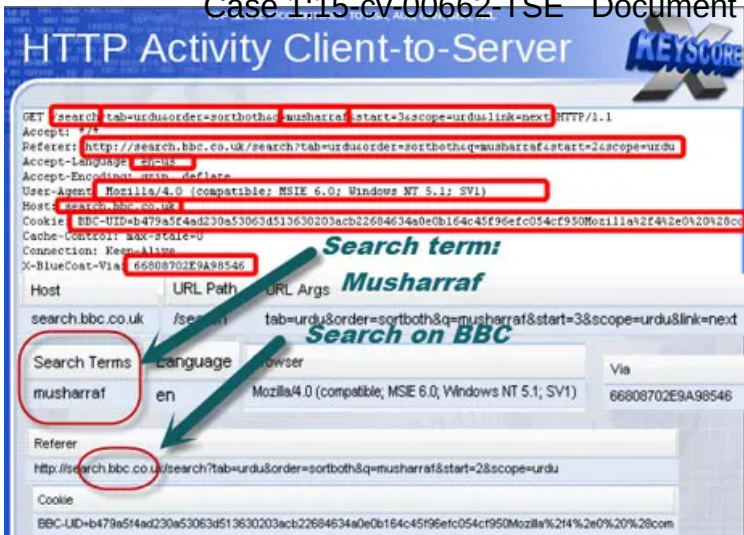
KS55edit Photograph: Guardian

An analyst can monitor such Facebook chats by entering the Facebook user name and a date range into a simple search screen.



KS6 Photograph: Guardian

Analysts can search for internet browsing activities using a wide range of information, including search terms entered by the user or the websites viewed.



KS7 Photograph: Guardian

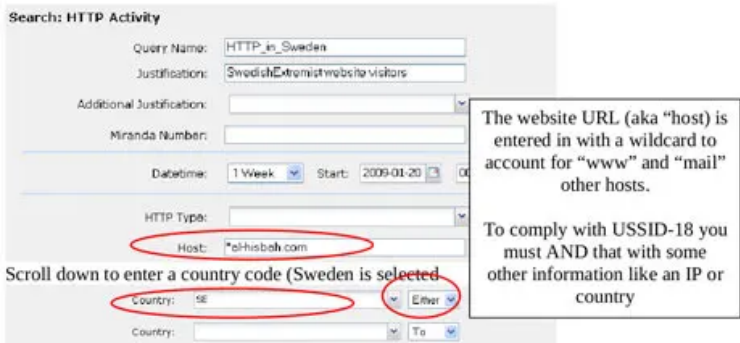
As one slide indicates, the ability to search HTTP activity by keyword permits the analyst access to what the NSA calls "nearly everything a typical user does on the internet".



KS8 Photograph: Guardian

The XKeyscore program also allows an analyst to learn the IP addresses of every person who visits any website the analyst specifies.

1. If you know the particular website the target visits. For this example, I'm looking for everyone in Sweden that visits a particular extremist web forum.



KS9 Photograph: Guardian

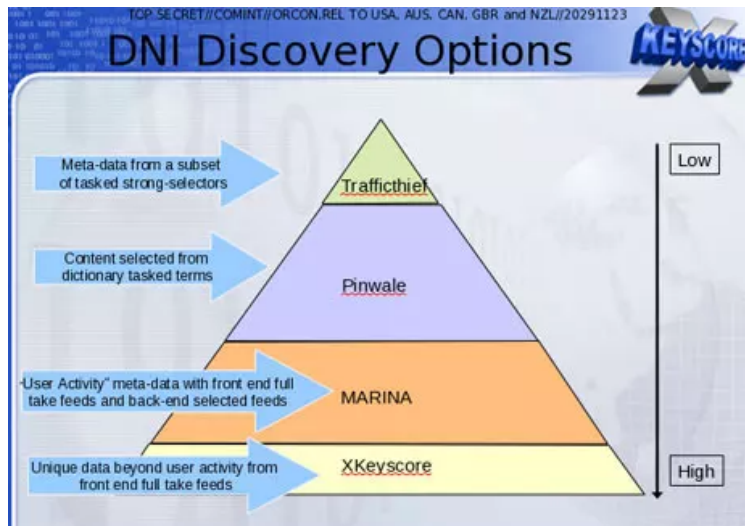
The quantity of communications accessible through programs such as XKeyscore is staggeringly large. One NSA report from 2007 estimated that there were 850bn "call events" collected and stored in the NSA databases, and close to 150bn internet records. Each day, the document says, 1-2bn records were added.

William Binney, a former NSA mathematician, said last year that the agency had "assembled on the order of 20tn transactions about US citizens with other US citizens", an estimate, he said, that "only was involving phone calls and emails". A 2010 Washington Post article reported that "every day, collection systems at the [NSA] intercept and store 1.7bn emails, phone calls and other type of communications."

The XKeyscore system is continuously collecting so much internet data that it can be stored only for short periods of time. Content remains on the system for only three to five days, while metadata is stored for 30 days. One document explains: "At some sites, the amount of data we receive per day (20+ terabytes) can only be stored for as little as 24 hours."

To solve this problem, the NSA has created a multi-tiered system that allows analysts to store "interesting" content in other databases, such as one named Pinwale which can store material for up to five years.

It is the databases of XKeyscore, one document shows, that now contain the greatest amount of communications data collected by the NSA.



KS10 Photograph: Guardian

In 2012, there were at least 41 billion total records collected and stored in XKeyscore for a single 30-day period.

### Legal v technical restrictions

While the Fisa Amendments Act of 2008 requires an individualized warrant for the targeting of US persons, NSA analysts are permitted to intercept the communications of such individuals without a warrant if they are in contact with one of the NSA's foreign targets.

The ACLU's deputy legal director, Jameel Jaffer, told the Guardian last month that national security officials expressly said that a primary purpose of the new law was to enable them to collect large amounts of Americans' communications without individualized warrants.





**XKEYSCORE**  
47,995,304,143  
Records

"The government doesn't need to 'target' Americans in order to collect huge volumes of their communications," said Jaffer. "The government inevitably sweeps up the communications of many Americans" when targeting foreign nationals for surveillance.

An example is provided by one XKeyscore document showing an NSA target in Tehran communicating with people in Frankfurt, Amsterdam and New York.

TOP SECRET//COMINT//REL TO USA, AUK, CAN, GBR, FRA

### Example #2

- Full Log table contains the standard DNI meta-data with *some but not all* information from other plug-ins included (ie. Username from User Activity and Application Info contains some HTTP activity)

Application Info	Username	Em IP	Em IP	To (City)	Destination	Em IP	Em IP	Em IP	Em IP	
http://update.nsl.com/Products.Cc		TEHRAN	US	NEWYORK	2009-05-20 18:05:41	2009-05-20 00:00:16			3842	00
http://platform.fb.facebook.com/v	narges.arastode@gmail.co	TEHRAN	DE	FRANKFURT	2009-05-20 18:05:41	2009-05-20 00:00:16			4206	00
http://platform.fb.facebook.com/v	narges.arastode@gmail.co	TEHRAN	DE	FRANKFURT	2009-05-20 18:05:41	2009-05-20 00:00:16			4206	00
http://platform.fb.facebook.com/v	narges.arastode@gmail.co	TEHRAN	DE	FRANKFURT	2009-05-20 18:05:41	2009-05-20 00:00:16			4206	00
http://news.us.abc.co.uk/younew		TEHRAN	GB	LONDON	2009-05-20 18:05:41	2009-05-20 00:00:16			3783	00
http://b.state.ak.fbcdn.net/track		TEHRAN	DE	FRANKFURT	2009-05-20 18:05:41	2009-05-20 00:00:16			4192	00
http://b.state.ak.fbcdn.net/track		TEHRAN	DE	FRANKFURT	2009-05-20 18:05:41	2009-05-20 00:00:16			4192	00
http://platform.fb.facebook.com/v	narges.arastode@gmail.co	TEHRAN	DE	FRANKFURT	2009-05-20 18:05:41	2009-05-20 00:00:16			4048	00
http://photos-dak.fbcdn.net/phot		TEHRAN	NL	AMSTERDAM	2009-05-20 18:05:41	2009-05-20 00:00:16			4151	00
http://photos-dak.fbcdn.net/phot		TEHRAN	NL	AMSTERDAM	2009-05-20 18:05:41	2009-05-20 00:00:16			4151	00

IP addresses redacted

KS12 Photograph: Guardian

In recent years, the NSA has attempted to segregate exclusively domestic US communications in separate databases. But even NSA documents acknowledge that such efforts are imperfect, as even purely domestic communications can travel on foreign systems, and NSA tools are sometimes unable to identify the national origins of communications.

Moreover, all communications between Americans and someone on foreign soil are included in the same databases as foreign-to-foreign communications, making them readily searchable without warrants.

Some searches conducted by NSA analysts are periodically reviewed by their supervisors within the NSA. "It's very rare to be questioned on our searches," Snowden told the Guardian in June, "and even when we are, it's usually along the lines of: 'let's bulk up the justification!'"

In a letter this week to senator Ron Wyden, director of national intelligence James Clapper acknowledged that NSA analysts have exceeded even legal limits as interpreted by the NSA in domestic surveillance.

Acknowledging what he called "a number of compliance problems", Clapper attributed them to "human error" or "highly sophisticated technology issues" rather than "bad faith".

However, Wyden said on the Senate floor on Tuesday: "These violations are more serious than those stated by the intelligence community, and are troubling."

In a statement to the Guardian, the NSA said: "NSA's activities are focused and specifically deployed against - and only against - legitimate foreign intelligence targets in response to requirements that our leaders need for information necessary to protect our nation and its interests."

"XKeyscore is used as a part of NSA's lawful foreign signals intelligence collection system."

"Allegations of widespread, unchecked analyst access to NSA collection data are simply not true. Access to XKeyscore, as well as all of NSA's analytic tools, is limited to only those personnel who require access for their assigned tasks ... In addition, there are multiple technical, manual and supervisory checks and balances within the system to prevent deliberate misuse from occurring."

"Every search by an NSA analyst is fully auditable, to ensure that they are proper and within the law."

"These types of programs allow us to collect the information that enables us to perform our missions successfully - to defend the nation and to protect US and allied troops abroad."

\$0  
contributed

\$0  
our goal

## **In these critical times ...**

... Guardian columnist and author Rebecca Solnit urges you to show your support for independent journalism with a year-end gift to The Guardian. We are asking our US readers to help us raise \$1 million dollars by the new year to report on the most important stories in 2019.

A note from Rebecca:

"First they came for the journalists," said the young man's sign. "We don't know what happened after that." It's a brilliant comment that underscores two things. One is how utterly necessary it is to a free, powerful, informed public, to have the ability to act on what happens beyond our own horizon, to make choices about our governments whether by blockading a senate or parliament or electing people we've learned about from the news.

The other is how much tyrants and would-be tyrants fear a free press - and what your enemies think is often the best way to measure whether you matter. They know autocracy depend on keeping the public ignorant on some fronts and misinformed on others.

We've seen direct attacks on journalists in the past year, from the murder of Jamal Khashoggi to Trump's incessant attacks on the media as "the enemy of the people," and for a couple of decades we've seen the indirect attacks that are Silicon Valley's siphoning off of advertising revenue and amplification of untruths for profit.

It costs a lot to send someone out to cover a campaign or to investigate a crime; it's hard work that requires expertise and support from our readers. This year, The Guardian has covered everything from tech to feminism to Trump to fossil fuel politics. It is our editorial independence that has

Case 1:15-cv-00662-TSE Document 168-31 Filed 12/18/18 Page 11 of 11  
allowed us to deliver this fearless reporting; an independence that's sometimes hard to find in other US-based media. We hope you appreciate our efforts.

We want to say a huge thank you to everyone who has supported The Guardian so far. We hope to pass our goal by early January 2019. Every contribution, big or small, will help us reach it. **Please make a year-end gift today to show your ongoing support for our independent journalism. Thank you.**

Support The Guardian



Topics

- The NSA files
- Glenn Greenwald on security and liberty
- Surveillance
- NSA
- Privacy
- Internet
- Data protection
- US politics
- news