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

Plaintiff's Exhibit 29

The Intercept_

XKEYSCORE

NSA's Google for the World's Private Communications

Morgan Marquis-Boire, Glenn Greenwald, Micah Lee

July 1 2015, 10:49 a.m.

One of the National Security Agency's most powerful tools of mass surveillance makes tracking someone's Internet usage as easy as entering an email address, and provides no built-in technology to prevent abuse. Today, *The Intercept* is publishing 48 top-secret and other classified documents about XKEYSCORE dated up to 2013, which shed new light on the breadth, depth and functionality of this critical spy system — one of the largest releases yet of documents provided by NSA whistleblower Edward Snowden.

The NSA's XKEYSCORE program, first revealed by *The Guardian*, sweeps up countless people's Internet searches, emails, documents, usernames and passwords, and other private communications. XKEYSCORE is fed a constant flow of Internet traffic from fiber optic cables that make up the backbone of the world's communication network, among other sources, for processing. As of 2008, the surveillance system boasted approximately 150 field sites in the United States, Mexico, Brazil, United Kingdom, Spain, Russia, Nigeria, Somalia, Pakistan, Japan, Australia, as well as many other countries, consisting of over 700 servers.

These servers store "full-take data" at the collection sites – meaning that they captured all of the traffic collected – and, as of 2009, stored content for 3 to 5 days and metadata for 30 to 45 days. NSA documents indicate that tens of billions of records are stored in its database. "It is a fully distributed processing and query system that runs on machines around the world," an NSA briefing on XKEYSCORE says. "At field sites, XKEYSCORE can run on multiple computers that gives it the ability to scale in both processing power and storage."

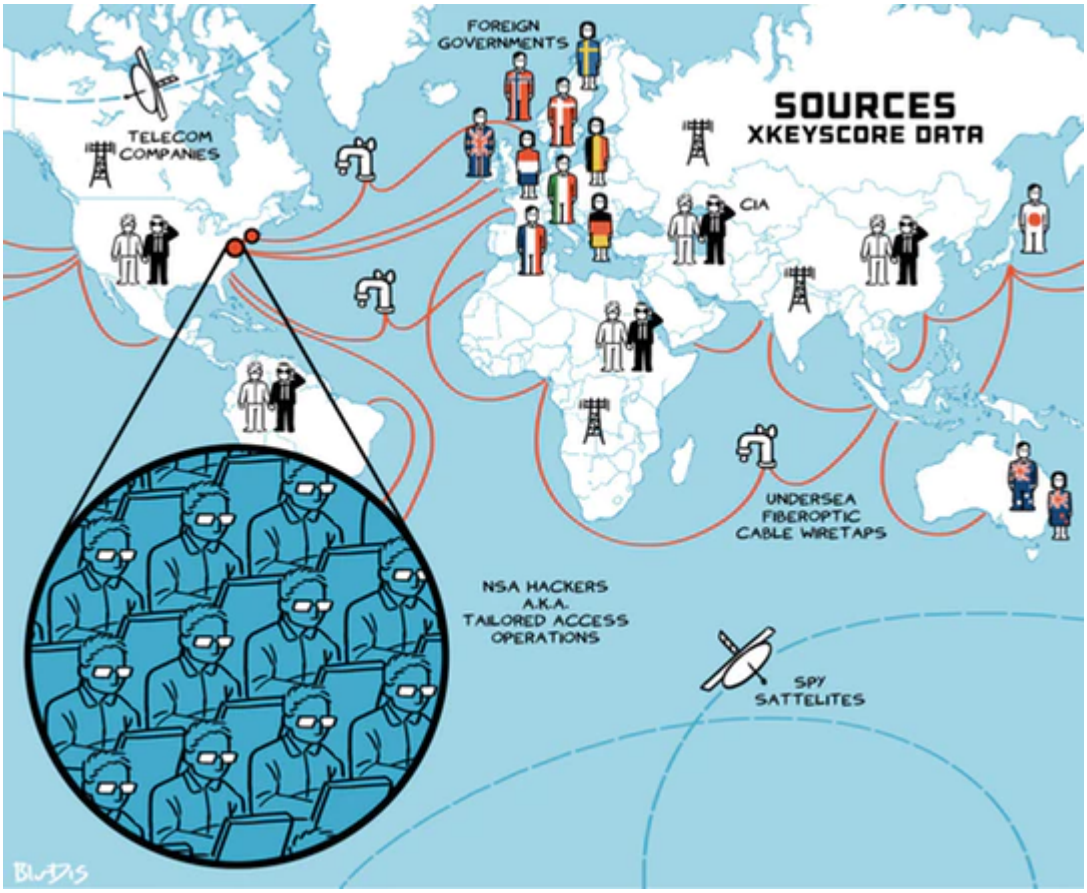

Illustration: Blue Delliquanti and David Axe for The Intercept

XKEYSCORE also collects and processes Internet traffic from Americans, though NSA analysts are taught to avoid querying the system in ways that might result in spying on U.S. data. Experts and privacy activists, however, have long doubted that such exclusions are effective in preventing large amounts of American data from being swept up. One document *The Intercept* is publishing today suggests that FISA warrants

have authorized "full-take" collection of traffic from at least some U.S. web forums.

The system is not limited to collecting web traffic. The 2013 document, "VoIP Configuration and Forwarding Read Me," details how to forward VoIP data from XKEYSCORE into NUCLEON, NSA's repository for voice intercepts, facsimile, video and "pre-released transcription." At the time, it supported more than 8,000 users globally and was made up of 75 servers absorbing 700,000 voice, fax, video and tag files per day.

The reach and potency of XKEYSCORE as a surveillance instrument is astonishing. The *Guardian* report noted that NSA itself refers to the program as its "widest reaching" system. In February of this year, *The Intercept* reported that NSA and GCHQ hacked into the internal network of Gemalto, the world's largest provider of cell phone SIM cards, in order to steal millions of encryption keys used to protect the privacy of cell phone communication. XKEYSCORE played a vital role in the spies' hacking by providing government hackers access to the email accounts of Gemalto employees.

Numerous key NSA partners, including Canada, New Zealand and the U.K., have access to the mass surveillance databases of XKEYSCORE. In March, the *New Zealand Herald*, in partnership with *The Intercept*, revealed that the New Zealand government used XKEYSCORE to spy on candidates for the position of World Trade Organization director general and also members of the Solomon Islands government.

These newly published documents demonstrate that collected communications not only include emails, chats and web-browsing traffic, but also pictures, documents, voice calls, webcam photos, web searches, advertising analytics traffic, social media traffic, botnet traffic, logged keystrokes, computer network exploitation (CNE) targeting, intercepted username and password pairs, file uploads to online services, Skype sessions and more.

Bulk collection and population surveillance

XKEYSCORE allows for incredibly broad surveillance of people based on perceived patterns of suspicious behavior. It is possible, for instance, to query the system to show the activities of people based on their location, nationality and websites visited. For instance, one slide displays the search "germansinpakistn," showing an analyst querying XKEYSCORE for all individuals in Pakistan visiting specific German language message boards.

As sites like Twitter and Facebook become increasingly significant in the world's day-to-day communications (a Pew study shows that 71 percent of online adults in the U.S. use Facebook), they become a critical source of surveillance data. Traffic from popular social media sites is described as "a great starting point" for tracking individuals, according to an XKEYSCORE presentation titled "Tracking Targets on Online Social Networks."

When intelligence agencies collect massive amounts of Internet traffic all over the world, they face the challenge of making sense of that data. The vast quantities collected make it difficult to connect the stored traffic to specific individuals.

Internet companies have also encountered this problem and have solved it by tracking their users with identifiers that are unique to each individual, often in the form of browser cookies. Cookies are small pieces of data that websites store in visitors' browsers. They are used for a variety of purposes, including authenticating users (cookies make it possible to log in to websites), storing preferences, and uniquely tracking individuals even if they're using the same IP address as many other people. Websites also embed code used by third-party services to

collect analytics or host ads, which also use cookies to track users. According to one slide, "Almost all websites have cookies enabled."

The NSA's ability to piggyback off of private companies' tracking of their own users is a vital instrument that allows the agency to trace the data it collects to individual users. It makes no difference if visitors switch to public Wi-Fi networks or connect to VPNs to change their IP addresses: the tracking cookie will follow them around as long as they are using the same web browser and fail to clear their cookies.

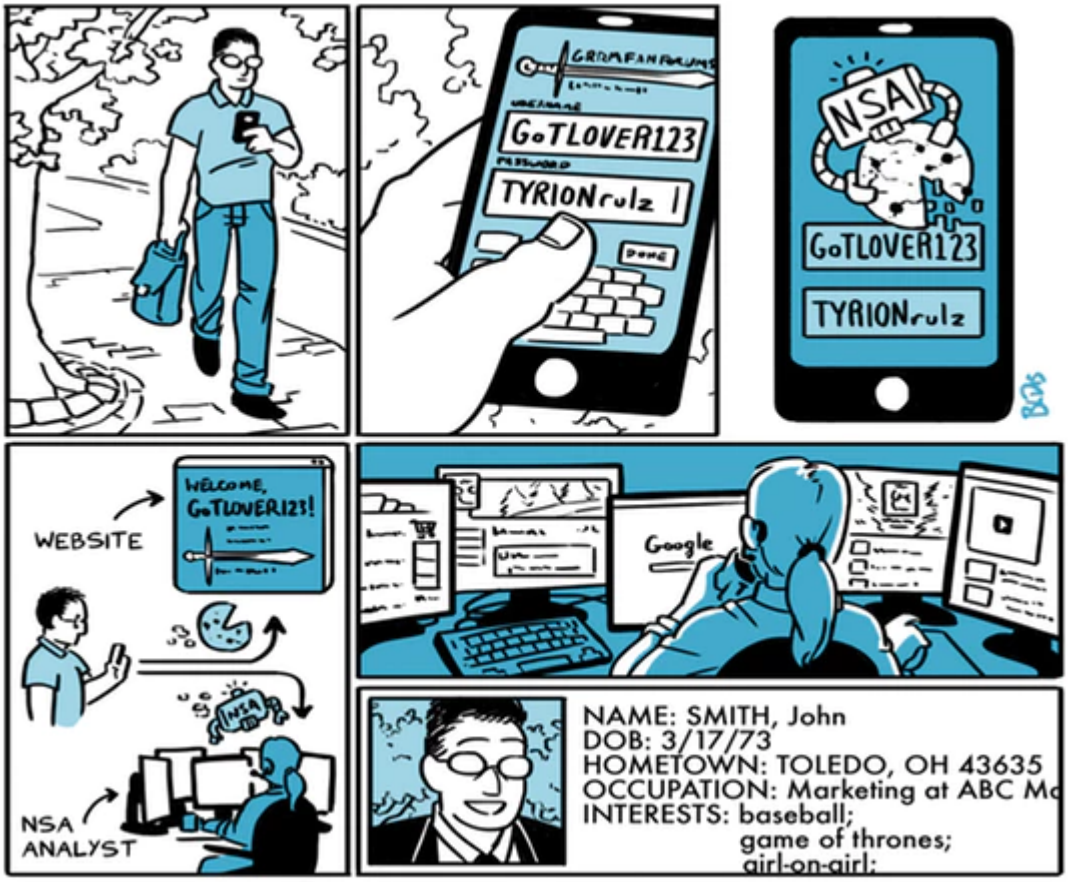

Illustration: Blue Delliquanti and David Axe for The Intercept

Apps that run on tablets and smartphones also use analytics services that uniquely track users. Almost every time a user sees an advertisement (in an app or in a web browser), the ad network is tracking users in the same way. A secret GCHQ and CSE program called BADASS, which is similar to XKEYSCORE but with a much narrower scope, mines as much valuable information from leaky smartphone

apps as possible, including unique tracking identifiers that app developers use to track their own users. In May of this year, CBC, in partnership with *The Intercept*, revealed that XKEYSCORE was used to track smartphone connections to the app marketplaces run by Samsung and Google. Surveillance agency analysts also use other types of traffic data that gets scooped into XKEYSCORE to track people, such as Windows crash reports.

In a statement to *The Intercept*, the NSA reiterated its position that such sweeping surveillance capabilities are needed to fight the War on Terror:

"The U.S. Government calls on its intelligence agencies to protect the United States, its citizens, and its allies from a wide array of serious threats. These threats include terrorist plots from al-Qaeda, ISIL, and others; the proliferation of weapons of mass destruction; foreign aggression against the United States and our allies; and international criminal organizations."

Indeed, one of the specific examples of XKEYSCORE applications given in the documents is spying on Shaykh Atiyatallah, an al Qaeda senior leader and Osama bin Laden confidant. A few years before his death, Atiyatallah did what many people have often done: He googled himself. He searched his various aliases, an associate and the name of his book. As he did so, all of that information was captured by XKEYSCORE.

XKEYSCORE has, however, also been used to spy on non-terrorist targets. The April 18, 2013 issue of the internal NSA publication Special Source Operations Weekly boasts that analysts were successful in using XKEYSCORE to obtain U.N. Secretary General Ban Ki-moon's talking points prior to a meeting with President Obama.

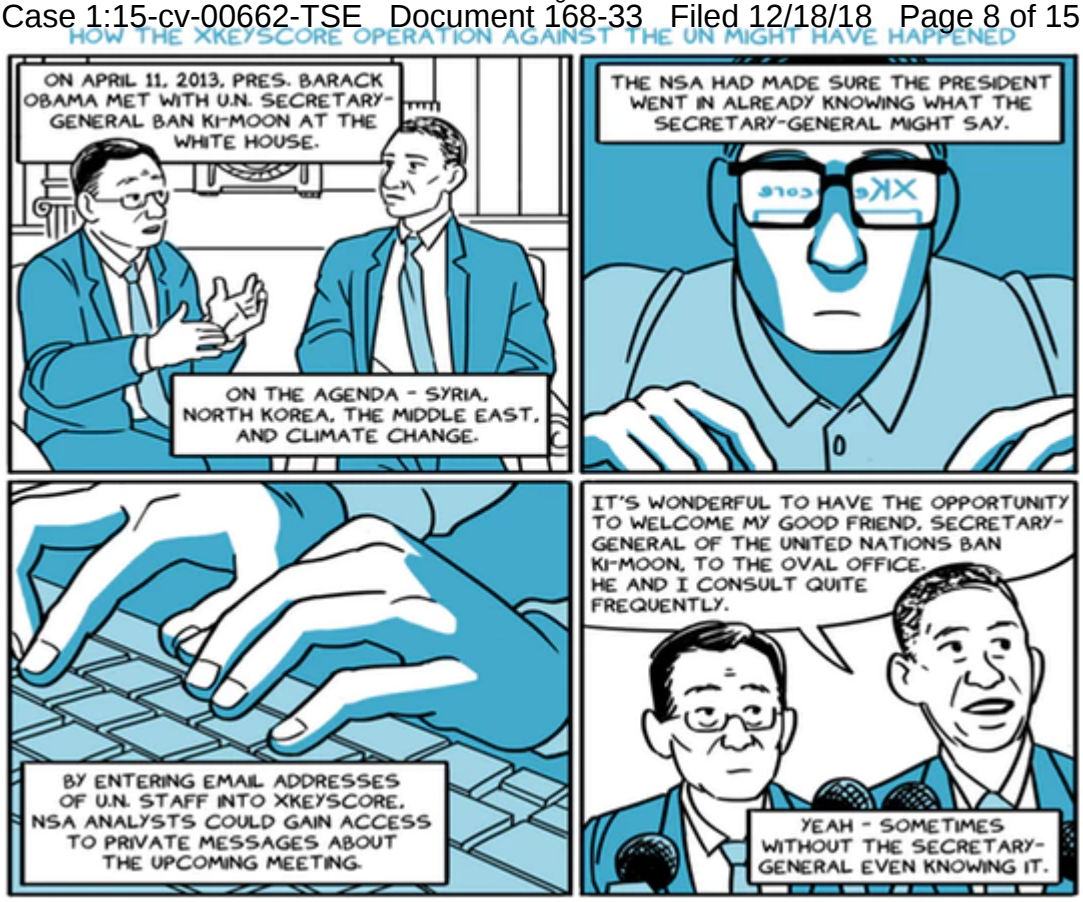

Illustration: Blue Delliquanti and David Axe for The Intercept

XKEYSCORE for hacking: Easily collecting user names, passwords and much more

XKEYSCORE plays a central role in how the U.S. government and its surveillance allies hack computer networks around the world. One top-secret 2009 NSA document describes how the system is used by the NSA to gather information for the Office of Tailored Access Operations, an NSA division responsible for Computer Network Exploitation (CNE) – i.e., targeted hacking.

Particularly in 2009, the hacking tactics enabled by XKEYSCORE would have yielded significant returns as use of encryption was less widespread than today. Jonathan Brossard, a security researcher and the

CEO of Toucan Systems, told *The Intercept*: "Anyone could be trained to do this in less than one day: they simply enter the name of the server they want to hack into XKEYSCORE, type enter, and are presented login and password pairs to connect to this machine. Done. Finito." Previous reporting by *The Intercept* revealed that systems administrators are a popular target of the NSA. "Who better to target than the person that already has the 'keys to the kingdom?'" read a 2012 post on an internal NSA discussion board.

This system enables analysts to access web mail servers with remarkable ease.

The same methods are used to steal the credentials — user names and passwords — of individual users of message boards.

Hacker forums are also monitored for people selling or using exploits and other hacking tools. While the NSA is clearly monitoring to understand the capabilities developed by its adversaries, it is also monitoring locations where such capabilities can be purchased.

Other information gained via XKEYSCORE facilitates the remote exploitation of target computers. By extracting browser fingerprint and operating system versions from Internet traffic, the system allows analysts to quickly assess the exploitability of a target. Brossard, the security researcher, said that "NSA has built an impressively complete set of automated hacking tools for their analysts to use."

Given the breadth of information collected by XKEYSCORE, accessing and exploiting a target's online activity is a matter of a few mouse clicks. Brossard explains: "The amount of work an analyst has to perform to actually break into remote computers over the Internet seems ridiculously reduced — we are talking minutes, if not seconds. Simple. As easy as typing a few words in Google."

These facts bolster one of Snowden's most controversial statements, made in his first video interview published by *The Guardian* on June 9, 2013. "I, sitting at my desk," said Snowden, could "wiretap anyone, from you or your accountant, to a federal judge to even the president, if I had a personal email."

Indeed, training documents for XKEYSCORE repeatedly highlight how user-friendly the program is: with just a few clicks, any analyst with access to it can conduct sweeping searches simply by entering a person's email address, telephone number, name or other identifying data. There is no indication in the documents reviewed that prior approval is needed for specific searches.

In addition to login credentials and other target intelligence, XKEYSCORE collects router configuration information, which it shares with Tailored Access Operations. The office is able to exploit routers and then feed the traffic traveling through those routers into their collection infrastructure. This allows the NSA to spy on traffic from otherwise out-of-reach networks. XKEYSCORE documents reference router configurations, and a document previously published by *Der Spiegel* shows that "active implants" can be used to "cop[y] traffic and direc[t]" it past a passive collector.

XKEYSCORE for counterintelligence

Beyond enabling the collection, categorization, and querying of metadata and content, XKEYSCORE has also been used to monitor the surveillance and hacking actions of foreign nation states and to gather the fruits of their hacking. *The Intercept* previously reported that NSA and its allies spy on hackers in order to collect what they collect.

Once the hacking tools and techniques of a foreign entity (for instance, South Korea) are identified, analysts can then extract the country's espionage targets from XKEYSCORE, and gather information that the foreign power has managed to steal.

Monitoring of foreign state hackers could allow the NSA to gather techniques and tools used by foreign actors, including knowledge of zero-day exploits – software bugs that allow attackers to hack into systems, and that not even the software vendor knows about – and implants. Additionally, by monitoring vulnerability reports sent to vendors such as Kaspersky, the agency could learn when exploits they were actively using need to be retired because they've been discovered by a third party.

Seizure v. searching: Oversight, audit trail and the Fourth Amendment

By the nature of how it sweeps up information, XKEYSCORE gathers communications of Americans, despite the Fourth Amendment protection against "unreasonable search and seizure" – including searching data without a warrant. The NSA says it does not target U.S. citizens' communications without a warrant, but acknowledges that it "incidentally" collects and reads some of it without one, minimizing the information that is retained or shared.

But that interpretation of the law is dubious at best.

XKEYSCORE training documents say that the "burden is on user/auditor to comply with USSID-18 or other rules," apparently including the British Human Rights Act (HRA), which protects the rights of U.K. citizens. U.S. Signals Intelligence Directive 18 (USSID 18) is the American directive that governs "U.S. person minimization."

Kurt Opsahl, the Electronic Frontier Foundation's general counsel, describes USSID 18 as "an attempt by the intelligence community to comply with the Fourth Amendment. But it doesn't come from a court, it comes from the executive."

If, for instance, an analyst searched XKEYSCORE for all iPhone users, this query would violate USSID 18 due to the inevitable American iPhone users that would be grabbed without a warrant, as the NSA's own training materials make clear.

Opsahl believes that analysts are not prevented by technical means from making queries that violate USSID 18. "The document discusses whether auditors will be happy or unhappy. This indicates that compliance will be achieved by after-the-fact auditing, not by preventing the search."

Screenshots of the XKEYSCORE web-based user interface included in slides show that analysts see a prominent warning message: "This system is audited for USSID 18 and Human Rights Act compliance." When analysts log in to the system, they see a more detailed message warning that "an audit trail has been established and will be searched" in response to HRA complaints, and as part of the USSID 18 and USSID 9 audit process.

Because the XKEYSCORE system does not appear to prevent analysts from making queries that would be in violation of these rules, Opsahl concludes that "there's a tremendous amount of power being placed in the hands of analysts." And while those analysts may be subject to audits, "at least in the short term they can still obtain information that they shouldn't have."

During a symposium in January 2015 hosted at Harvard University, Edward Snowden, who spoke via video call, said that NSA analysts are "completely free from any meaningful oversight." Speaking about the

people who audit NSA systems like XKEYSCORE for USSID 18 compliance, he said, "The majority of the people who are doing the auditing are the friends of the analysts. They work in the same office. They're not full-time auditors, they're guys who have other duties assigned. There are a few traveling auditors who go around and look at the things that are out there, but really it's not robust."

In a statement to *The Intercept*, the NSA said:

"The National Security Agency's foreign intelligence operations are 1) authorized by law; 2) subject to multiple layers of stringent internal and external oversight; and 3) conducted in a manner that is designed to protect privacy and civil liberties. As provided for by Presidential Policy Directive 28 (PPD-28), all persons, regardless of their nationality, have legitimate privacy interests in the handling of their personal information. NSA goes to great lengths to narrowly tailor and focus its signals intelligence operations on the collection of communications that are most likely to contain foreign intelligence or counterintelligence information."

Coming next: A Look at the Inner Workings of XKEYSCORE

Source maps: XKS as a SIGDEV Tool, p. 15, and XKS Intro, p. 6

Documents published with this article:

- Advanced HTTP Activity Analysis
- Analyzing Mobile Cellular DNI in XKS
- ASFD Readme
- CADENCE Readme
- Category Throttling
- CNE Analysis in XKS
- Comms Readme

- DEEPDIVE Readme
- DNI101
- Email Address vs User Activity
- Free File Uploaders
- Finding and Querying Document Metadata
- Full Log vs HTTP
- Guide to Using Contexts in XKS Fingerprints
- HTTP Activity in XKS
- HTTP Activity vs User Activity
- Intro to Context Sensitive Scanning With XKS Fingerprints
- Intro to XKS AppIDs and Fingerprints
- OSINT Fusion Project
- Phone Number Extractor
- RWC Updater Readme
- Selection Forwarding Readme
- Stats Config Readme
- Tracking Targets on Online Social Networks
- TRAFFICTHIEF Readme
- Unofficial XKS User Guide
- User Agents
- Using XKS to Enable TAO
- UTT Config Readme
- VOIP in XKS
- VOIP Readme
- Web Forum Exploitation Using XKS
- Writing XKS Fingerprints
- XKS Application IDs
- XKS Application IDs Brief
- XKS as a SIGDEV Tool
- XKS, Cipher Detection, and You!
- XKS for Counter CNE
- XKS Intro

- XKS Logos Embedded in Docs
- XKS Search Forms
- XKS System Administration
- XKS Targets Visiting Specific Websites
- XKS Tech Extractor 2009
- XKS Tech Extractor 2010
- XKS Workflows 2009
- XKS Workflows 2011
- UN Secretary General XKS