The Shocking Scope of the NSA's XKEYSCORE Surveillance

Every time anyone uses a computer to send an e-mail, watch a video, do a Google search, or update a Facebook status, the National Security Agency (NSA) is probably collecting and collating that activity on one of its many servers.

XKEYSCORE — the codename of the computer code used by the NSA to perform these actions — is massive and more intrusive than most people understand.

On July 2, Micah Lee, Glenn Greenwald, and Morgan Marquis-Boire of *The Intercept* published the [second of a two-part exposé](#) of the inner-workings of this system that should shock the consciences of constitutionalists and civil libertarians.

The revelations are based on information gleaned from documents leaked to Greenwald (and others) by Edward Snowden, the former NSA contractor turned whistleblower who uncovered and then revealed the massive violations of the Constitution being carried out by the government of the United States.

How wide is the net cast by the NSA's XKEYSCORE system? *The Intercept* reports:

> 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.

Surprisingly, the second installment reveals that XKEYSCORE is powerful, despite being built on some rather simple software. *The Intercept* reports:

> This global Internet surveillance network is powered by a somewhat clunky piece of software running on clusters of Linux servers. Analysts access XKEYSCORE's web interface to search its wealth of private information, similar to how ordinary people can search Google for public information.

> It is tempting to assume that expensive, proprietary operating systems and software must power XKEYSCORE, but it actually relies on an entirely open source stack. In fact, according to an analysis of an XKEYSCORE manual for new systems administrators from the end of 2012, the system may have design deficiencies that could leave it vulnerable to attack by an intelligence agency insider.

> XKEYSCORE is a piece of Linux software that is typically deployed on Red Hat servers. It uses the Apache web server and stores collected data in MySQL databases. File systems in a cluster are handled by the NFS distributed file system and the autofs service, and scheduled tasks are handled by the cron scheduling service. Systems administrators who maintain XKEYSCORE servers use SSH to connect to them, and they use tools such as rsync and vim, as well as a comprehensive

command-line tool, to manage the software.

While the vulnerabilities of the NSA's XKEYSCORE system are disturbing, the way it is used to gobble up gigabytes of personal data and online habits of millions of people never suspected of any crime should certainly be more alarming.

Greenwald first described the details of the program in July 2013 after examining a PowerPoint presentation included in the information he received from Snowden. In his first report, he explained the scope of XKEYSCORE.

> One presentation claims the [XKEYSCORE] 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.

Exactly how does it work? Greenwald explained that, too: "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. 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."

The New American published information earlier that the NSA uses XKEYSCORE to save gigabytes of Internet traffic data; however, that is a gross understatement.

According to the *Intercept* report:

> As of 2009, XKEYSCORE servers were located at more than 100 field sites all over the world. Each field site consists of a cluster of servers; the exact number differs depending on how much information is being collected at that site. Sites with relatively low traffic can get by with fewer servers, but sites that spy on larger amounts of traffic require more servers to filter and parse it all. XKEYSCORE has been engineered to scale in both processing power and storage by adding more servers to a cluster. According to a 2009 document, some field sites receive over 20 terrabytes of data per day. This is the equivalent of 5.7 million songs, or over 13 thousand full-length films.

That's how much personal information is collected — without a warrant — every single day.

It's not just the content of e-mails and Facebook posts; XKEYSCORE allows NSA operators to steal user names and passwords and to monitor and download the complete content of "Facebook chat messages and pull out details like the associated email address and body of the chat message."

There are those who insist that only data relevant to tracking and capturing (read: killing with a drone) suspected terrorists are actually examined by the NSA. That's not what these latest documents reveal, however.

These servers store "full-take data" at the collection sites — meaning that they capture all 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."

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 published by *The Intercept* suggests that FISA warrants have authorized "full-take" collection of traffic from at least some U.S. web forums.

That's right. The secret FISA Court (the one that recently nullified an act of Congress and rebooted the NSA's surveillance servers) often gives the spies the green light to gobble up and analyze the personal Internet data of American citizens living in America. All of which, of course, is unconstitutional without a warrant.

Readers need to have in the front of their minds the standard to which the federal government must be held.

The Fourth Amendment to the Constitution mandates:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

As these latest documents demonstrate, for over a decade our elected representatives (and the courts, for that matter) have disregarded the Constitution and built a domestic spy apparatus that bears no resemblance whatsoever to the blueprint provided by our Founding Fathers in the Constitution.

Finally, it should be pointed out that many of the documents described by Greenwald and his colleagues at *The Intercept* are from 2009. That isn't to imply that the program has ended, but rather that over the last six years it has likely become bigger, more insidious, and more intrusive.