Nach einem Bericht in der britischen Zeitung The Guardian kann die NSA mit ihrem Programm XKeyscore alle Internetaktivitäten jedes beliebigen Nutzers ohne richterliche Genehmigung überwachen.

LUFTPOST

Friedenspolitische Mitteilungen aus der US-Militärregion Kaiserslautern/Ramstein
LP 108/13 – 04.08.13

XKeyscore: Ein NSA-Tool verschafft Zugang "zu fast allem, was ein Nutzer im Internet tut"

Von Glen Greenwald
The Guardian, 31.07.13
(http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data/print)

XKeyscore ermöglicht die weitreichendste Sammlung von Online-Daten
NSA-Analysten brauchen keine Genehmigung für Nachforschungen mit XKeyscore
XKeyscore ermöglicht den Zugriff auf E-Mails, Aktivitäten in sozialen Netzwerken und alle Suchvorgänge im Internet
Eine Präsentation zum XKeyscore-Programm der NSA ist aufzurufen unter
http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation

Ein streng geheimes Programm der National Security Agency / NSA ermöglicht Analysten ohne vorherige Genehmigung den Zugriff auf riesengroße Datenbanken – auf E-Mails, Online Chats und Internet-Suchvorgänge von Millionen Nutzern; das geht aus Dokumenten hervor, die Whistleblower Edward Snowden zur Verfügung gestellt hat.

Rote Punkte zeigen, wo XKeyscore eingesetzt wird

Der NSA prahlt in einer Präsentation für Lehrzwecke damit, dass dieses Programm mit dem Namen XKeyscore (den man als "Universal-Zugriffsberechtigung" eindeutschen könnte) "das weitreichendste System zur geheimdienstlichen Ausforschung des Internets" sei.

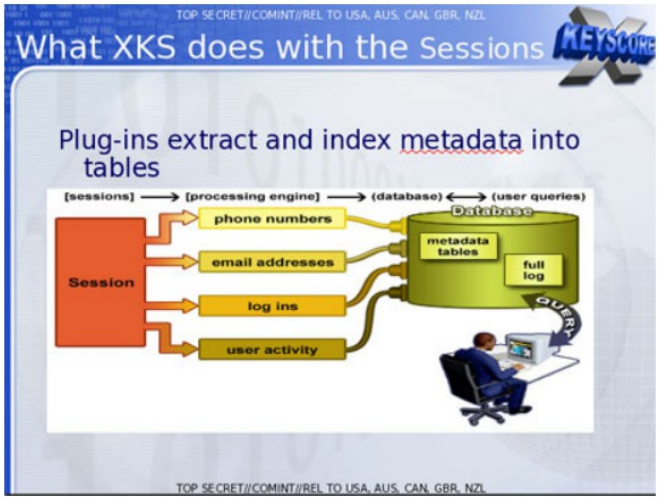
Die jüngsten Enthüllungen werden die heftigen Debatten in der Öffentlichkeit und im US-Kongress über das Ausmaß der NSA-Überwachungsprogramme (s. http://www.theguardian.com/world/surveillance) weiter anheizen. Sie wurden am Mittwoch veröffentlicht, während führende Geheimdienstleute vom Rechtsausschuss des Senats zu früheren Veröffentlichungen des *Guardian* über die massenhafte Aufzeichnung von Telefonanrufen [s. unter http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order] und andere Überwachungsmaßnahmen im Rahmen des Foreign Intelligence Surveillance Act / FISA (s. http://de.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act) befragt wurden.

Die neuen Dokumente werfen Licht auf eine der aufsehenerregendsten Erklärungen aus Snowdens ersten Videointerview, das der *Guardian* am 10. Juni veröffentlicht hat [s. http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order].

Snowden sagte damals: "Von meinem Schreibtisch aus konnte ich jeden anzapfen – Sie selbst, Ihren Steuerberater, einen Bundesrichter oder sogar den Präsidenten – jede Person, von der ich eine persönliche E-Mail-Adresse hatte."

US-Offizielle widersprachen dieser Behauptung besonders vehement. Mike Rogers, der republikanische Vorsitzende des Geheimdienstausschusses des Repräsentantenhauses, sagte dazu: "Snowden lügt. Was er da behauptet, konnte er unmöglich tun."

Aus Lehrmaterialien für das XKeyscore-Programm geht hervor, wie Analysten dieses und andere Systeme nutzen können, um sich durch Ausfüllen eines einfachen Online-Formulars mit einer sehr allgemein gehaltenen Begründung für ihre Recherche Zugang zu riesigen Datensammlungen der NSA zu verschaffen. Die Anfrage muss nicht von einem Gericht oder einem NSA-Vorgesetzten genehmigt werden.



Bei Internetaktivitäten abgegriffene Metadaten

In den Dokumenten wird damit geprahlt, dass XKeyscore "das weitreichendste System" der NSA zu geheimdienstlichen Überwachung von Computer-Netzwerken sei; man nennt das Digital Network Intelligence / DNI (digitale Netzwerk-Ausforschung). Auf einer Präsentationstafel wird behauptet, das Programm ermögliche den Zugriff auf "fast alles, was ein typischer Nutzer im Internet tut" – auch auf den Inhalt von E-Mails, auf Suchvorgänge im Internet und die dazugehörenden Meta-Daten.

Analysten können XKeyscore und andere NSA-Systeme auch zur längeren Überwachung der Internetaktivitäten einer Person in Echtzeit verwenden.

Nach US-Recht braucht die NSA bei FISA-Überwachungen nur dann eine richterliche Genehmigung, wenn die Zielperson ein "US-Amerikaner" ist; die Genehmigung entfällt aber, ist, wenn US-Amerikaner mit Ausländern kommunizieren. XKeyscore bietet die technologischen Möglichkeiten zur umfassenden elektronischen Kontrolle von US-Amerikanern auch dann, wenn keine richterliche Genehmigung vorliegt, der Analyst aber die E-Mail-Adresse der Zielperson oder die IP-Adresse (des mit dem Internet verbundenen Geräts) kennt.

Aus einer Lehrtafel der Präsentation geht hervor, dass der Analyst mit XKeyscore Internetaktivitäten einzelner Personen auch ständig überwachen und Datenbanken jederzeit anzapfen kann.

Mit XKeyscore können Analysten sowohl die Metadaten als auch den Inhalt von E-Mails und andere Internetaktivitäten wie Suchvorgänge überwachen, selbst wenn ihnen die Internetadresse einer Zielperson, die im NSA-Jargon "Selector" (Zugang) genannt wird, nicht bekannt ist.

Analysten können auch Namen, Telefonnummern, IP-Adressen oder Schlüsselwörter in der Sprache, in der die Internetaktivität stattfindet, als Suchkriterien benutzen oder einen bestimmten Browser-Typ ausforschen.

In einem (NSA-)Dokument wird das damit begründet, dass [die Suche über die E-Mail-

Adresse] nur begrenzte Möglichkeiten biete, weil "ein großer Teil der im Web unternommenen Aktivitäten anonym erfolgt".

In NSA-Dokumenten wird behauptet, dass 2008 durch die Überwachung mit XKeystore 300 Terroristen festgenommen werden konnten.

Die Analysten werden vor einer Durchsuchung der gesamten Datenbank gewarnt, weil dabei zu viele Hinweise anfielen, die überprüft werden müssten. Stattdessen wird ihnen empfohlen, von den ebenfalls in Datenbanken gespeicherten Metadaten auszugehen, weil die zu überprüfende Datenmenge dann geringer sei.

Auf einer Präsentationstafel mit dem Titel "Plug-Ins" aus einem im Dezember 2012 entstandenen Dokument sind die verschiedenen Informationsfelder benannt, die durchsucht werden können. Erwähnt werden "alle E-Mail-Adressen, die bei einer Session (der Überwachung eines Internet-Nutzers) gefunden werden – einschließlich der User-Namen und der Domains", "jede bei einer Session erfasste Telefonnummer [auch aus Adressbüchern oder Unterschriftenlisten]" und andere Nutzeraktivitäten, wie "Webmails und Chats mit Nutzernamen, Freundeslisten, speziellen Cookies usw.".

E-Mail-Überwachung

In einem zweiten Interview, das der *Guardian* im Juni mit Snowden geführt hat, ging dieser ausführlich auf seine Behauptung ein, dass er die E-Mails beliebiger Personen mitlesen konnte, wenn er ihre E-Mail-Adresse hatte. Dazu hätten ihn vor allem die Funktionen von XKeyscore zur Durchsuchung von E-Mails befähigt, die er als Mitarbeiter der Firma Booz Allen (s. http://de.wikipedia.org/wiki/Booz_Allen_Hamilton), die im Auftrag der NSA arbeitet, zur Verfügung hatte.

Ein streng geheimes Dokument beschreibt, wie XKeyscore bei "E-Mails, Websites und (aufgerufenen) Dokumenten" außer "dem Empfänger und dem Absender auch die unter, CC und BCC aufgeführten Adressaten" und die Besucher einer Website registriert, die "Contact us" aufrufen.

Wenn ein XKeyscore benutzender Analyst E-Mails durchsuchen will, gibt er die E-Mail-Adresse der betreffenden Person in ein einfaches Online-Suchformular ein und fügt neben einer kurzen "Begründung" auch den Zeitraum ein, in dem er die E-Mails überprüfen will.

Der Analyst wählt dann aus, welche der (von XKeyscore) ausgesonderten E-Mails er lesen will; die kann er dann mit einen speziellen NSA-Software öffnen.

Das System ähnelt dem, mit dem NSA-Analysten auch auf andere (elektronische) Kommunikationsformen jeder ausgewählten Person zugreifen können, wenn die Botschaft – wie aus dem NSA-Dokument hervorgeht – die USA durchquert oder dort empfangen wird.

Ein Dokument aus einer streng geheimen Anleitung aus dem Jahr 2010, mit deren Hilfe NSA-Analysten die Durchführung von Überwachungsmaßnahmen nach den Vorschriften des Fisa Amendments Act von 2008 (Infos dazu sind aufzurufen unter http://en.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act_of_1978_Amendments_Act_of_2008 .) trainiert haben, erläutert, wie Analysten mit der Überwachung jeder beliebigen Person beginnen können: Sie müssen nur einige einfache Pulldown-Menüs (s. https://de.wikipedia.org/wiki/Dropout-Men%C3%BC) anklicken, aus denen sie rechtliche und personenbezogene Gründe für die Überwachung der Zielperson auswählen können. Sobald sie ihre Auswahl getroffen haben, ist die Person als Zielobjekt zur elektronischen Überwachung

freigegeben, und der Analyst kann dann den Inhalt ihrer gesamten elektronischen Kommunikation überprüfen.

Die Überwachung von Chats, Suchvorgängen und andere Internetaktivitäten

Außer E-Mails können Analysten mit dem System XKeyscore praktisch auch alle anderen Internetaktivitäten überwachen, einschließlich der in sozialen Netzwerken.

Mit einem NSA-Tool, das als DNI Presenter bezeichnet und zum Lesen gespeicherter E-Mails verwendet wird, kann ein Analyst, der XKeyscore verwendet, auch den Inhalt von Facebook-Chats oder privaten Nachrichten mitlesen.

Ein Analyst kann Facebook-Chats mitlesen, wenn er den Namen des Facebook-Nutzers und einen Zeitrahmen in ein einfaches Suchformular eingibt.

Analysten können auch Internetrecherchen nachvollziehen, indem sie die von dem Nutzer eingegebenen Suchbegriffe und die aufgerufenen Websites auswerten.

Eine Präsentationstafel belegt, dass der Analyst durch die Überwachung von HTTP-Aktivitäten (s. http://de.wikipedia.org/wiki/HTTP-Statuscode) per Schlüsselwort nach Angaben der NSA "Zugang zu fast allem erhält, was ein typischer Nutzer im Internet tut".

Mit Hilfe des XKeyscore-Programms kann ein Analyst auch die IP-Adressen (s. https://de.wikipedia.org/wiki/IP-Adresse) jeder Person erfahren, die eine beliebige Website besucht, die der Analytiker angibt.

Die Menge der Kommunikationsdaten, die mit Programmen wie XKeyscore abgegriffen werden können, ist unvorstellbar groß. In einem NSA-Bericht aus dem Jahr 2007 wird die Anzahl der mitgeschnittenen und in NSA-Datenbanken gespeicherten Telefonanrufe mit 850 Milliarden angegeben; im gleichen Zeitraum wurden fast 150 Milliarden Internetvorgänge aufgezeichnet. Aus dem Dokument ist auch ersichtlich, dass täglich 1 bis 2 Milliarden Datenaufzeichnungen dazu kommen.

William Binney, ein ehemaliger NSA-Mathematiker, hat im letzten Jahr mitgeteilt, die NSA habe nach Schätzungen rund 20 Billionen Daten über die (elektronische) Kommunikation zwischen US-Bürgern aufgezeichnet, und dabei handle es sich nur um Telefonanrufe und E-Mails. Die *Washington Post* hat 2010 berichtet, die NSA greife und speichere jeden Tag 1,7 Milliarden E-Mails, Anrufe und andere Kommunikationsvorgänge ab.

Das XKeyscore-System greift fortlaufend so viele Internetdaten ab, dass sie nur für kurze Zeitspannen gespeichert werden können. Die Inhalte bleiben in dem System nur für 3 bis 5 Tage verfügbar, die Metadaten werden 30 Tage gespeichert. Ein Dokument enthüllt: "Bei einigen Websites fällt täglich eine Datenmenge von 20 Terabytes und mehr an, die wir deshalb nur 24 Stunden speichern können."

Um dieses Problem zu beheben, hat die NSA ein mehrstufiges System geschaffen, das Analysten die Möglichkeit gibt, "interessante Inhalte" in anderen Datenbanken, zum Beispiel in einer namens Pinwale (könnte als "Pinnwand" eingedeutscht werden) abzuspeichern, wo das Material bis zu fünf Jahre lang verfügbar bleibt.

Aus einem anderen Dokument geht aber hervor, dass in den XKeyscore-Datenbanken die meisten der von der NSA gesammelten Kommunikationsdaten abgespeichert sind.

2012 wurden mindestens 41 Milliarden Datensätze abgegriffen und für jeweils 30 Tage in in XKeyscore-Datenbanken gespeichert.

Der Konflikt zwischen gesetzlichen Einschränkungen und technischen Möglichkeiten

Der Fisa Amendments Act / FISA von 2008 schreibt zwar für die Überwachung jedes einzelnen US-Bürgers eine richterliche Genehmigung vor, NSA-Analysten könne die Kommunikation von US-Bürgern aber trotzdem ohne Erlaubnis ausforschen, wenn diese Kontakt zu einer NSA-Zielperson im Ausland haben.

Jameel Jaffer, der für Rechtsfragen zuständige stellvertretende Direktor der American Civil Liberties Union / ACLU (s. http://de.wikipedia.org/wiki/American_Civil_Liberties_Union), äußerte letzten Monat gegenüber dem *Guardian*, Vertreter des NSA hätten zugegeben, FISA sei hauptsächlich beschlossen worden, um der NSA die Möglichkeit zum Überwachen von US-Bürgern ohne richterliche Genehmigung zu verschaffen.

"Die Regierung muss nicht unbedingt US-Amerikaner 'ins Visier nehmen', um an ganz viele ihrer Kommunikationsdaten zu kommen," erklärte Jaffer. "Auch wenn sie offiziell nur Ausländer überwachen lässt, fallen ihr jede Menge Kommunikationsdaten von US-Amerikanern in die Hände."

Ein Beispiel dafür liefert ein XKeyscore-Dokument, das den Kommunikationsfluss zwischen einer NSA-Zielperson in Teheran und Leuten in Frankfurt, Amsterdam und New York darstellt.

In den letzten Jahren hat die NSA versucht, reine US-Kommunikationsdaten in eigenen Datenbankern zu erfassen. Aus NSA-Dokumenten geht aber hervor, dass diese Bemühungen vergeblich waren, weil auch nur auf die USA beschränkter Datenverkehr über ausländische Übermittlungssysteme laufen kann; sogar mit den NSA-Tools lässt sich manchmal nicht feststellen, woher Daten ursprünglich kommen.

Außerdem werden auch alle Kommunikationsvorgänge zwischen US-Amerikanern und Ausländern in den gleichen Datenbanken abgespeichert wie die Kommunikationsvorgänge zwischen Ausländern untereinander und können daher ohne richterliche Genehmigung jederzeit herausgefischt werden.

Einige von NSA-Analysten durchgeführte Überwachungsaktionen werden gelegentlich von ihren NSA-Vorgesetzten überprüft. "Wir wurden aber nur sehr selten, zu unseren Überwachungsaktionen befragt," teilte Snowden im Juni dem *Guardian* mit, "und wenn das geschehen ist, wurde nur gefragt, ob wir uns auch an die vorgegebenen 'Begründungen' gehalten hätten."

James Clapper, der Director of National Intelligence (der Direktor der nationalen Nachrichtendienste, s. http://de.wikipedia.org/wiki/Director_of_National_Intelligence und http://www.luftpost-kl.de/luftpost-archiv/LP_13/LP08113_110613.pdf) hat diese Woche in einem Brief an Senator Ron Wyden sogar zugegeben, dass NSA-Analysten die von der NSA bereits sehr locker gehandhabten gesetzlichen Bestimmungen nicht eingehalten haben.

Clapper bestätigte zwar "mehrere Regelverstöße", erklärte sie aber zu "menschlichen oder aus der komplizierten Überwachungstechnologie erwachsenen Irrtümern", die "nicht aus böser Absicht" erfolgt seien.

Am Dienstag reagierte Wyden im Senat auf Clappers Brief mit folgender Feststellung: "Diese Übertretungen sind schwerwiegender, als von den Geheimdiensten behauptet wird, und sehr beunruhigend."

In einer an der *Guardian* adressierten Stellungnahme erklärte die NSA: "Die Aktivitäten der NSA richten sich ausdrücklich und ausschließlich gegen geheimdienstlich relevante Zielpersonen im Ausland; damit erfüllen wir den Auftrag unserer Regierung, ihr Informationen zu beschaffen, die sie zur Sicherung unserer Nation und unserer Interessen braucht.

XKeyscore ist ein Teil des gesetzlich legitimierten Systems der NSA zur nachrichtendienstlichen Informationsbeschaffung im Ausland.

Anschuldigungen, die NSA sammle und analysiere weltweit riesige Datenmengen, sind einfach nicht wahr. Der Zugang zu XKeyscore und allen anderen analytischen NSA-Tools ist auf Personen beschränkt, die sie zur Bewältigung der ihnen erteilten Aufträge unbedingt benötigen … . Außerdem gibt es vielfältige technische und manuelle Kontrollen, um einen vorsätzlichen Missbrauch des Systems zu verhindern.

Jeder Überwachungsauftrag eines NSA-Analysten ist prüffähig, um sicherzustellen, das er korrekt und nach gesetzlichen Vorschriften erfolgt.

Diese Art von Überwachungsprogrammen ermöglicht es uns, die Information zu sammeln, die wir zur erfolgreichen Durchführung unseres Auftrages benötigen – zur Verteidigung unserer Nation und zum Schutz der Truppen der USA und unserer Verbündeten bei ihren Auslandseinsätzen."

(Wie haben den Artikel, der die Bundestagsabgeordneten aller Parteien und die Bundesregierung noch vor der Wahl aufrütteln und zum sofortigen Einschreiten gegen die unerträgliche, flächendeckende, völkerrechts- und verfassungswidrige Überwachung der Bürger der souveränen Bundesrepublik Deutschland veranlassen sollte, komplett übersetzt und mit Ergänzungen und Links in runden Klammern versehen. Die Ergänzungen und Links in eckigen Klammern hat der Autor selbst eingefügt. Anschließend drucken wir den Originaltext ab.)

---

theguardian

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

Glenn Greenwald
31 July 2013

• 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

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

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 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 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:

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.

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

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

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".

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

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.

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.

"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.

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."

www.luftpost-kl.de
VISDP: Wolfgang Jung, Assenmacherstr. 28, 67659 Kaiserslautern