Aus einem der Washington Post zugespielten Geheimdokument geht hervor, dass der US-Abhörgeheimdienst NSA und sein britisches Gegenstück GCHQ direkten Zugriff auf die Server und damit auch auf die Nutzerdaten führender US-Provider haben.

LUFTPOST

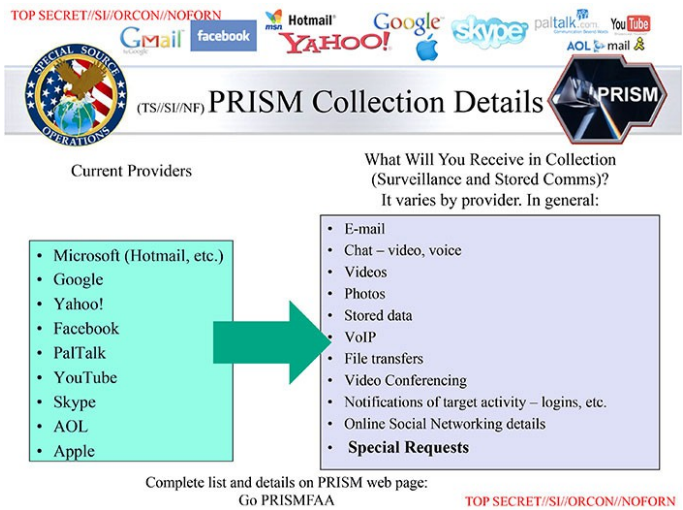
Friedenspolitische Mitteilungen aus der US-Militärregion Kaiserslautern/Ramstein
LP 080/13 – 10.06.13

Geheimdienste der USA und Großbritanniens greifen insgeheim in großem Umfang Daten von neun führenden US-Povidern ab

Von Barton Gellman und Laura Poitras
The Washington Post, 06./07.06.13
(http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html)

Die National Security Agency / NSA (Infos dazu sind aufzurufen unter http://de.wikipedia.org/wiki/National_Security_Agency) und das FBI greifen direkt von den zentralen Servern neun führender US-Provider nicht nur Audio- und Videochats, Fotos, E-Mails, und Dokumente, sondern auch Verbindungsdaten ab, damit ihre Analysten auch Zielpersonen im Ausland aufspüren und überwachen können; das geht aus einem streng geheimen Dokument hervor, das der *Washington Post* vorliegt.

Über das Programm mit dem Code-Namen PRISM (Prisma, s. http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/) war vorher noch nichts in die Öffentlichkeit gedrungen. Es könnte das erste seiner Art sein. Die NSA ist stolz darauf, Geheimnisse stehlen und Codes knacken zu können, und findet immer wieder Partner, die ihr helfen, den Datenverkehr umzulenken oder Hindernisse zu umgehen. Zwar hat es Google und Facebook früher noch nicht gegeben, aber es ist eher unwahrscheinlich, dass Geheimdienste dort wertvollere Funde als im Silicon Valley machen können.



Überwachte Provider (Alle Grafiken wurden entnommen aus http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/)

Auf welch ungewöhnliche Art sich die NSA die gewünschten Daten verschafft ist dem (nebenstehenden) Geheimdokument zu entnehmen: "Durch direkten Zugriff auf die Server der US-Provider Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube und Apple."

Die Londoner Zeitung *The Guardian* hat am Freitag berichtet, das Government Communications Headquarters / GCHQ, das britische Gegenstück zur NSA, habe sich durch Vermittlung der NSA ebenfalls insgeheim Zugriff auf die Daten der gleichen Provider verschaffen können.

Nach Dokumenten, die dem *Guardian* vorliegen, umgeht das GCHQ mit dem Programm PRISM das in Großbritannien vorgeschriebene formelle Genehmigungsverfahren, das not-

wendig ist, bevor persönliche Materialien wie E-Mails, Fotos und Videos eingesehen werden dürfen, indem es sich die Daten im Ausland besorgt.

PRISM ist aus der Asche eines geheimen, ungenehmigten Abhörprogramms des Präsidenten George W. Bush auferstanden, das 2007 von Medien enthüllt und vom Foreign Intelligence Suveillance Court (s. http://de.wikipedia.org/wiki/United_States_Foreign_Intelligence_Surveillance_Court) untersagt worden war; Bush musste sich deshalb nach einer anderen Möglichkeit umsehen.

Die verschaffte ihm der Kongress mit dem Protect America Act von 2007 (dem Gesetz zum Schutz der USA, s. http://en.wikipedia.org/wiki/Protect_America_Act_of_2007) und dem FISA Amendments Act von 2008 (dem Zusatzgesetz zum Gesetz über die Überwachungstätigkeit der US-Geheimdienste im Ausland, weitere Infos dazu unter http://en.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act_of_1978_Amendments_Act_of_2008); mit letzterem werden private Firmen dazu ermuntert, die US-Geheimdienste "freiwillig" bei der Sammlung von Informationen zu unterstützen. PRISM rekrutierte mit Microsoft seinen ersten Partner und sammelte bis heute eine riesige Menge Daten ein, obwohl die hitzige Debatte über Praktiken der Überwachung und den Schutz der Privatsphäre nie abriss. Als gegen Ende letzten Jahres Kritiker im Kongress den FISA Amendments Act ändern wollten, wurden die wenigen Abgeordneten und Senatoren, die über PRISM Bescheid wussten per Amtseid verpflichtet, den Mund zu halten.

Überwachte Datenströme

Das gerichtlich genehmigte Programm dient zur Überwachung des Datenverkehrs auf der ganzen Welt; der wird häufig über US-Server abgewickelt – selbst dann, wenn er sich ausschließlich im Ausland (zum Beispiel zwischen zwei Internet-Nutzern in der Bundesrepublik Deutschland) abspielt. Zwischen 2004 und 2007 haben es Bushs Rechtsanwälte geschafft, mit dem Foreign Intelligence Surveillance Court (einem US-Sondergericht, das für die Überwachung der Aktivitäten der US-Geheimdienste im Ausland zuständig ist, s. http://de.wikipedia.org/wiki/United_States_Foreign_Intelligence_Surveillance_Court) ein neues, sehr großzügiges Genehmigungsverfahren zu vereinbaren. Vorher musste die Regierung jeweils belegen, dass eine ganz bestimmte "Zielperson" oder "Einrichtung" Verbindungen zum Terrorismus oder zur Spionage hatte.

In vier neuen Verfügungen, die immer noch geheim gehalten werden, weitete das Gericht die Anzahl der zu überwachenden "Einrichtungen" stark aus und überprüft jetzt nur noch gelegentlich, ob die Regierung die Überwachung des Datenverkehrs von "US-Bürgern" ohne Einzelgenehmigung in angemessenem Ausmaß betreibt.

Letzten Donnerstag gab James R. Clapper, der Direktor der Nationalen Geheimdienste (s. http://de.wikipedia.org/wiki/Director_of_National_Intelligence) folgende Erklärung ab: "Die mit diesem Programm gesammelten Informationen gehören zu den wichtigsten und wertvollsten Erkenntnissen, die unsere Geheimdienste im Ausland sammeln, und sie tragen dazu bei, unsere Nation vor vielen, ganz unterschiedlichen Bedrohungen zu schützen. Die unautorisierte Enthüllung von Informationen über dieses wichtige und völlig legale Programm ist zu verurteilen, weil sie wichtige Schutzvorkehrungen für die Sicherheit von US-Amerikanern gefährdet."

Clapper fügte hinzu, in den Berichten der *Washington Post* und des *Guardian* über PRISM gebe es zahlreiche Ungenauigkeiten, wollte aber keine nennen.

Jameel Jaffer, der für Rechtsangelegenheiten zuständige stellvertretende Direktor der American Civil Liberties Union / ACLU (der Bürgerrechtsunion der USA, s. http://de.wikipedia.org/wiki/American_Civil_Liberties_Union) sagte: "Ich weise die Behauptung zurück, dass man sich keine Sogen machen müsse, weil ein Gericht das alles erlaubt hat. Dieses Gericht (der Foreign Intelligence Surveillance Court) tagt geheim, lässt nur Regierungsvertreter zu seinen Verhandlungen zu und veröffentlicht seine Entscheidungen höchst selten. Es hat noch nie eine wirksame Kontrolle über die Regierung ausgeübt."

Mehrere von der *Washington Post* befragte Provider erklärten, sie hätten keine Kenntnis von dem Programm gehabt und der Regierung auch nie den direkten Zugriff auf ihre Server erlaubt; sie behaupteten, nur bei gezielten Einzelanfragen Information weitergegeben zu haben.

"Wir haben keiner Regierungsorganisation den direkten Zugriff auf Facebook-Server erlaubt," betonte Joe Sullivan, der Chef-Sicherheitsbeauftragte bei Facebook. "Wenn Facebook um Daten oder Information über spezielle Personen gebeten wird, überprüfen wir bei jeder diesbezügliche Anfrage sorgfältig, ob sie nach den einschlägigen Gesetzen zulässig ist und geben auch nur die Informationen weiter, die ein Gesetz vorschreibt."

"Wir haben noch nie etwas von PRISM gehört," behauptete Steve Dowling, ein Sprecher des Apple-Konzerns. "Wir gestatten keiner Regierungsbehörde den direkten Zugriff auf unsere Server; jede Behörde, die Kundendaten von uns haben will, muss einen Gerichtsbeschluss vorlegen."

Es ist möglich, dass die Unterschiede zwischen den Angaben auf den PRISM-Grafiken und den Aussagen der Firmensprecher das Ergebnis verschleiernder NSA-Anforderungen sind. Einem anderen Geheimpapier, das der *Washington Post* auch vorliegt, ist zu entnehmen, dass der Zugriff auf Daten auch über andere von den Firmen betriebene Einrichtungen und nicht nur direkt über ihre Server erfolgen kann.

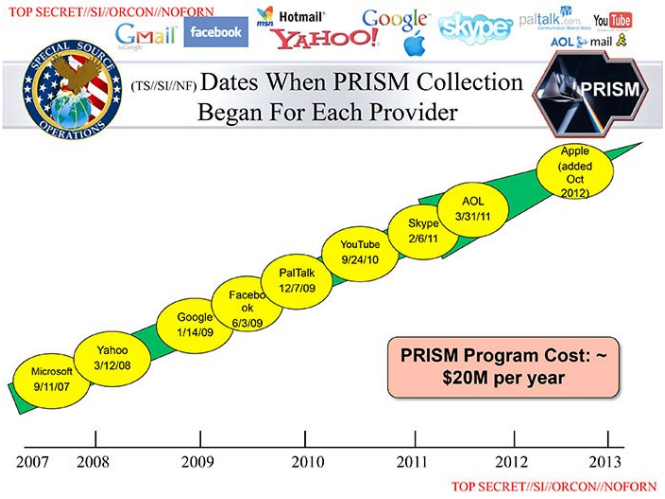
Aus Angaben von Regierungsvertretern und aus dem Dokument selbst geht hervor, dass die NSA die Identität ihrer privaten Partner als das heikelste Geheimnis des PRISM-Programms gehütet hat, weil sie den Rückzug der Provider aus dem Programm befürchten muss, falls deren Beteiligung bekannt wird. "98 Prozent der durch PRISM abgegriffenen Daten stammen von Yahoo, Google und Microsoft; wir müssen sicherstellen, dass wir diese Quellen nicht in Schwierigkeiten bringen," schrieb der Autor der Präsentation (aus der die Grafiken stammen) in den Notizen zu seinem Vortrag.

Die PRISM-Präsentation besteht aus 41 Grafiken und wurde im April 2013 zur internen Information für führende Analysten des Signals Intelligence Direcorate erstellt .(s. http://nolet.com/tags/organization/nsas-signals-intelligence-directorate); darin wird der Datenklau als produktivste Quelle für das Geheimdienst-Dossier bezeichnet, das Präsident Obama täglich vorgelegt wird. Der Präsident hat im letzten Jahr 1.477-mal aus der PRISM-Datensammlung zitiert. Aus der Präsentation und anderen der *Washington Post* zugespielten Materialien geht hervor, "dass sich jeder siebte NSA-Bericht auf das PRISM-Programm als Hauptquelle für Rohdaten stützt".

Das ist eine bemerkenswerte Zahl für einen Geheimdienst, der jährlich Billionen mitgeschnittener Nachrichten auswertet. Sie ist noch erstaunlicher, wenn berücksichtigt wird dass die NSA, die eigentlich ein Auslandsgeheimdienst ist, Datenspeicher von in den USA

ansässigen Firmen kontrolliert, bei denen auch Hunderte von Millionen US-Amerikaner Nutzerkonten haben.

Nach Angaben in dem Geheimdokument gehören zu den Providern, die mit PRISM kooperieren, die meisten der dominierenden Global Player im Silicon Valley. Auf einem Pfeil werden sie in der Reihenfolge ihrer Aufnahme in das PRISM-Programm aufgeführt: "Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL, Apple." Über den relativ kleinen Provider PalTalk liefen ein großer Teil der Internet-Kommunikation während des Arabischen Frühlings und der Datenaustausch im noch andauernden syrischen Bürgerkrieg.



Beginn der Überwachung bei den jeweiligen Providern

Der Datenspeicherungs- und Synchronisationsservice Dropbox (Infos dazu s. http://de.wikipedia.org/wiki/Dropbox), soll "bald noch dazukommen".

Die Senatoren Ron Wyden, ein Demokrat aus Oregon, und Mark Udall, ein Demokrat aus Colorado, die als Mitglieder des Geheimdienstausschusses des Senats Kenntnis von dem PRISM-Programm hatten, durften darüber aber nicht sprechen, als sie am 27. Dezember 2012 in einer Generaldebatte vor dem FISA Amendments Act (s. S. 2) warnten; beide nannten das Gesetz "ein verborgenes Hintertürchen", weil es Suchaktionen erlaube, durch die auch unbescholtene US-Bürger ausspioniert werden könnten.

"Nach dem vorliegenden Gesetzestext kann niemand die Geheimdienste daran hindern, haufenweise Kommunikationsdaten zu durchsuchen, die ohne richterliche Genehmigung zufällig oder versehentlich gesammelt wurden, um bewusst Telefonanrufe oder E-Mails bestimmter US-Bürger herauszufiltern," warnte Udall.

Wyden hat die NSA wiederholt aufgefordert, die Anzahl der US-Bürger zu schätzen, deren Kommunikationsdaten zufällig gesammelt wurden, aber Lt. Gen. (Generalleutnant) Keith B. Alexander, der Direktor der NSA, beteuerte immer wieder, dass dies nicht möglich sei. Schließlich schrieb der NSA-Generalinspekteur I. Charles McCullough III (s. http://www.nsa.gov/about/oig/oig_hotline.shtml) an Wyden einen Brief, in dem er ihm mitteilte, wenn die NSA Auskunft über die geschätzte Anzahl der ihren Datenbanken erfassten US-Bürger gebe, verletze das deren Privatsphäre.

Die Wurzeln des PRISM-Programms liegen in den 70er Jahren

PRISM ist in gewisser Hinsicht aus der Zusammenarbeit der Geheimdienste mit rund 100 vertrauenswürdigen US-Firmen erwachsen, die seit den 1970er Jahren stattfindet. Die NSA fasst diese Kooperation unter der Bezeichnung "Special Source Operations" (Operationen mit besonderen Quellen) zusammen, und PRISM fällt auch unter diese Rubrik.

Neben der Operation Silicon Valley (mit dem Code-Namen PRISM) läuft ein paralleles Programm mit dem Code-Namen BLARNEY, mit dem "Metadaten" (s. http://de.wikipedia.org/wiki/Metadaten) – das sind technische Informationen über den Kommunikationsverkehr und Netzwerk-Verbindungen – gesammelt werden, die an Choke Points (Engpässen, s. http://docstore.mik.ua/orelly/networking_2ndEd/fire/ch03_03.htm in Datenübertra-

gungsleitungen des Internets abgegriffen werden. Informationen über das streng geheime BLARNEY-Programm befinden sich auf Grafiken, auf denen eine Karikatur mit einem Kleeblatt und einer Heinzelmännchen-Mütze zu sehen ist; es wird als "ein ohne Unterbrechung laufendes Sammelprogramm bezeichnet, das sich mit Unterstützung (befreundeter) Geheimdienste und kommerzieller Partner Zugang zu Erkenntnissen zu verschaffen versucht, die Geheimdienste anderer (nicht verbündeter) Staaten in globalen Netzwerken gewonnen haben".

Das PRISM-Programm gehört wohl zu den umstrittensten Kontrollmaßnahmen, die ohne richterliche Überwachung stattfinden und nach den Al-Qaida-Anschlägen am 11. September 2001 von Präsident George W. Bush eingeführt wurden. Unter Präsident Obama wurden die Überwachungsmaßnahmen, die der Kandidat Obama noch heftig kritisiert hatte, stark ausgeweitet – von der Überwachung einzelner verdächtiger Individuen zur systematischen Durchforstung und Auswertung riesiger Datenströme.

Die Regierung Obama verweist immer wieder auf umfassende, von Gerichten geprüfte Schutzvorkehrungen, die sicherstellen sollen, dass nur Ausländer außerhalb der USA ins Visier genommen werden, während die beiläufig anfallenden Informationen über US-Bürger in nur sehr geringem Ausmaß gesammelt, gespeichert und ausgewertet würden.

Tatsächlich arbeitet das PRISM-Programm nicht wie ein Schleppnetz (das alles einsammelt). Aus dem Datenstrom eines Providers könnte die NSA jeweils alles herausfiltern, was sie interessiert, nach den gegenwärtig geltenden Vorschriften darf sie das aber (eigentlich) nicht.

Analysten, die das Programm von einem Webportal in Fort Meade in Maryland aus durchführen, benützen "Schlüsselwörter" als Suchbegriffe, die so ausgewählt werden, dass mindestens 51 Prozent der herausgefischten Nachrichten von ausländischen Nutzern stammen. Die Auswahl ist also nicht besonders "zielgerichtet". Aus Trainingsmaterialien, die der *Washington Post* ebenfalls vorliegen, geht hervor, dass Anfänger unter den Analysten vierteljährlich über zufällig aufgefangene Nachrichten von US-Bürgern Bericht erstatten, "sich deshalb aber keine Sorgen machen müssen".

Selbst wenn das Auswahlverfahren so zuverlässig – und wie angegeben – nicht auf US-Bürger ausgerichtet wäre, sammelt die NSA trotzdem routinemäßig sehr viel aus den USA stammendes Datenmaterial. Das wird zwar als "Zufall" ausgegeben, es ist aber unvermeidlich, weil die Verfolgung von Kommunikationsketten zum Handwerkszeug von Geheimdiensten gehört. Wer Informationen über einen mutmaßlichen Spion oder ausländischen Terroristen sammelt, muss sich mindesten auch um die Absender von E-Mails kümmern, die der Verdächtige erhält, und um die Empfänger von E-Mails, die der Verdächtige versendet. Geheimdienstanalysten sind angewiesen, die Kontakte des Verdächtigen – von ihm aus gesehen – "mindestens zweistufig" zu überprüfen (also auch andere Kontakte der Empfänger und Absender seiner E-Mails auszuforschen); das lässt die "zufällige Datensammlung" exponentiell (immer schneller) anwachsen. Die gleiche mathematische Regel gilt auch für das "Kleine-Welt-Phänomen", dass jeder Mensch über nur sechs Stufen mit jedem anderen Menschen irgendwie verbunden ist – wie es John Guare in seinem Stück "Six Degrees of Separation" (s. http://en.wikipedia.org/wiki/Six_Degrees_of_Separation_%28play%29) aufgezeigt hat.

Eine "Weisung"

Im Austausch gegen zugesicherte Straffreiheit (bei eigentlich strafbarem Verhalten) mussten sich Provider wie Yahoo und AOL dazu verpflichten, auf Weisung des Justizministers

oder des Direktors der nationalen Geheimdienste der "Data Intercept Technology Unit" des FBI den Zugriff auf ihre Server zu gestatten; diese FBI-Spezialeinheit stellt die Verbindung zwischen den US-Providern und der NSA her. 2008 hat der Kongress das Justizministerium dazu ermächtigt, Provider, die nicht kooperieren wollen, durch einen Beschluss des Gerichts, das die Auslandstätigkeit der Geheimdienste überwacht, zur Zusammenarbeit zu "veranlassen".

In der praktischen Zusammenarbeit hätte ein Provider trotzdem die Möglichkeit, den Zugriff auf seinen Server zu erschweren, zu verzögern oder zu verweigern. Wenn ein Geheimdienst mit einem verdeckt eingesetzten Programm in die hochtechnisierte Datenübermittlung eingreifen will, kann nach Meinung eines Rechtsanwaltes, der Erfahrung mit der Überbrückung von Interessengegensätzen hat, keine Seite eine öffentliche Auseinandersetzung riskieren. Die technischen Probleme sind bei Systemen, die so komplex sind und sich so häufig ändern, so gewaltig, dass das FBI und die NSA in große Schwierigkeiten kämen, wenn sie sich ohne aktive Unterstützung der Provider den Zugriff auf die Daten durch eine Hintertür selbst verschaffen müssten.

Apple hat gezeigt, dass Widerstand möglich ist, denn der Konzern hat aus unbekannten Gründen länger als fünf Jahre jede Kooperation verweigert; Microsoft wurde schon 2007 der erste Kooperationspartner im PRISM-Programm. Twitter hat den Ruf, die Privatsphäre seiner Nutzer sehr aggressiv zu verteidigen, und fehlt wohl deshalb noch auf der Liste der privaten Kooperationspartner.

Google hat – wie andere Provider auch – bestritten, der US-Regierung einen direkten Zugriff auf seine Server erlaubt zu haben.

"Google tut alles, um die Daten seiner Benutzer zu schützen," sagte ein Firmensprecher. "Wir geben Benutzerdaten nur dann an die Regierung heraus, wenn wir gesetzlich dazu verpflichtet sind, und wir überprüfen alle Anfragen sehr sorgfältig. Immer wieder wird behauptet, wir hätten der Regierung eine 'Hintertür' in unser System geöffnet, aber bei Google gibt es keine Hintertür, durch die sich die Regierung einen Zugang zu privaten Benutzerdaten (von US-Bürgern) verschaffen könnte."

Auch Microsoft hat eine Erklärung abgegeben: "Wir stellen Kundendaten nur dann zur Verfügung, wenn wir unter Strafandrohung gerichtlich dazu verpflichtet werden und werden das niemals auf freiwilliger Basis tun. Außerdem geben wir nur dann Auskunft, wenn sich die Anfrage auf ein genau benanntes Nutzerkonto oder eindeutige Identifizierungsmerkmale bezieht. Wenn die Regierung ein breiter angelegtes Programm zur Erhaltung der nationalen Sicherheit betreibt, um damit Kundendaten zu sammeln, sind wir jedenfalls nicht daran beteiligt."

Und Yahoo streitet jegliche Beteiligung ab.

"Yahoo nimmt die Privatsphäre seiner Nutzer sehr ernst," ließ der Provider erklären. "Wir gestatten der Regierung keinen direkten Zugriff auf unsere Server, unsere Systeme oder unser Netzwerk."

Wie Marktforscher, aber über einen Zugang mit viel mehr Privilegien, können sich die Datensammler in der "Special Source Operations Group" der NSA (in der operativen Gruppe der NSA für spezielle Quellen), die das PRISM-Programm betreut, aus dem reichen Datenbestand in den Nutzerkonten der Überwachten bedienen. Deshalb sind Bürgerrechtler und sicher auch einige normale Nutzer sehr besorgt über die vielfältigen Auswertungsmöglichkeiten, die Analysten mit Zugangsberechtigung zum PRISM-Programm haben.

Nach Aussagen in den PRISM-Grafiken ist die Auswertung von Facebook- und Skype-Konten "exponentiell gewachsen". Mit wenigen Klicks und einer Bestätigung, dass die zu überwachende Person vermutlich etwas mit Terrorismus, Spionage oder der Verbreitung von Atomwaffen zu tun hat, erhält ein Analyst vollen Zugriff auf die umfangreichen Such- und Kontrollmöglichkeiten, die Facebook im Vergleich mit anderen sozialen Netzwerken im Internet bietet.

Aus einem eigenen "Benutzerhandbuch des PRISM-Programms für die Skype-Auswertung" geht hervor, dass bei Bedarf auch Tonübermittlungen mitgehört werden können, wenn ein Gesprächsteilnehmer ein konventionelles Telefon benutzt; außerdem ist das Mithören auch "bei jeder Art von Audio-, Video-, Chat- und sonstigen Tonübertragungen" möglich, wenn Skype-Nutzer sie über ihre Computer abwickeln. Google bietet ja auch G-Mails, Gesprächs- und Videochats, Google Drive Files (Infos dazu s. http://www.basicthinking.de/blog/2012/04/24/google-drive-ist-da-ordentlich-als-cloud-speicher-besser-als-moderne-office-variante-und-als-filesharing-client/) Foto-Bibliotheken und die Live-Überwachung von Suchvorgängen an.

Eigene Erfahrungen mit dem PRISM-Programm und Entsetzen über die Möglichkeiten, die es eröffnet hat, haben einen Offizier, der beim Geheimdienst Karriere gemacht hat, dazu getrieben, der *Washington Post* die PowerPoint-Grafiken über das PRISM-Programm und die Begleitmaterialien zur Verfügung zu stellen, weil er die ungeheuren Eingriffe in die Privatsphäre publik machen möchte. "Die können tatsächlich schon mitlesen, wenn Sie Ihre Ideen in Ihre Tastatur eintippen," warnte der Offizier.

Laura Poitras ist eine Dokumentarfilmerin, die von der MacArthur-Stiftung ausgezeichnet wurde. Auch Julie Tate, Robert O'Harrow Jr., Cecilia Kang und Ellen Nakashima haben zu diesem Bericht beigetragen.

(Wir haben den Artikel komplett übersetzt und mit Ergänzungen und Links in Klammern versehen. Jetzt ist also erwiesen, was schon immer vermutet wurde: Der "Freund" hört und sieht alles mit – und Obama findet das auch noch gut und richtig, wie unter http://www.nytimes.com/2013/06/08/us/national-security-agency-surveillance.html?emc=na&_r=0 zu sehen und zu hören ist, weil ja bevorzugt ausländische Internet-Nutzer ausspioniert werden. Anschließend drucken wir den Originaltext ab.)

The Washington Post

U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program

By Barton Gellman and Laura Poitras,
Published: June 6 | Updated: Friday, June 7

The National Security Agency and the FBI are tapping directly into the central servers of nine leading U.S. Internet companies, extracting audio and video chats, photographs, e-mails, documents, and connection logs that enable analysts to track foreign targets, according to a top-secret document obtained by The Washington Post.

The program, code-named PRISM, has not been made public until now. It may be the first of its kind. The NSA prides itself on stealing secrets and breaking codes, and it is accusto-

med to corporate partnerships that help it divert data traffic or sidestep barriers. But there has never been a Google or Facebook before, and it is unlikely that there are richer troves of valuable intelligence than the ones in Silicon Valley.

Equally unusual is the way the NSA extracts what it wants, according to the document: “Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple.”

London’s Guardian newspaper reported Friday that GCHQ, Britain’s equivalent of the NSA, also has been secretly gathering intelligence from the same internet companies through an operation set up by the NSA.

According to documents obtained by The Guardian, PRISM would appear to allow GCHQ to circumvent the formal legal process required in Britain to seek personal material such as emails, photos and videos from an internet company based outside of the country.

PRISM was launched from the ashes of President George W. Bush’s secret program of warrantless domestic surveillance in 2007, after news media disclosures, lawsuits and the Foreign Intelligence Surveillance Court forced the president to look for new authority.

Congress obliged with the Protect America Act in 2007 and the FISA Amendments Act of 2008, which immunized private companies that cooperated voluntarily with U.S. intelligence collection. PRISM recruited its first partner, Microsoft, and began six years of rapidly growing data collection beneath the surface of a roiling national debate on surveillance and privacy. Late last year, when critics in Congress sought changes in the FISA Amendments Act, the only lawmakers who knew about PRISM were bound by oaths of office to hold their tongues.

The court-approved program is focused on foreign communications traffic, which often flows through U.S. servers even when sent from one overseas location to another. Between 2004 and 2007, Bush administration lawyers persuaded federal FISA judges to issue surveillance orders in a fundamentally new form. Until then the government had to show probable cause that a particular “target” and “facility” were both connected to terrorism or espionage.

In four new orders, which remain classified, the court defined massive data sets as “facilities” and agreed to certify periodically that the government had reasonable procedures in place to minimize collection of “U.S. persons” data without a warrant.

In a statement issue late Thursday, Director of National Intelligence James R. Clapper said “information collected under this program is among the most important and valuable foreign intelligence information we collect, and is used to protect our nation from a wide variety of threats. The unauthorized disclosure of information about this important and entirely legal program is reprehensible and risks important protections for the security of Americans.”

Clapper added that there were numerous inaccuracies in reports about PRISM by The Post and the Guardian newspaper, but he did not specify any.

Jameel Jaffer, deputy legal director of the American Civil Liberties Union, said: “I would just push back on the idea that the court has signed off on it, so why worry? This is a court that meets in secret, allows only the government to appear before it, and publishes almost none of its opinions. It has never been an effective check on government.”

Several companies contacted by The Post said they had no knowledge of the program, did not allow direct government access to their servers and asserted that they responded only to targeted requests for information.

“We do not provide any government organization with direct access to Facebook servers,” said Joe Sullivan, chief security officer for Facebook. “When Facebook is asked for data or information about specific individuals, we carefully scrutinize any such request for compliance with all applicable laws, and provide information only to the extent required by law.”

“We have never heard of PRISM,” said Steve Dowling, a spokesman for Apple. “We do not provide any government agency with direct access to our servers, and any government agency requesting customer data must get a court order.”

It is possible that the conflict between the PRISM slides and the company spokesmen is the result of imprecision on the part of the NSA author. In another classified report obtained by The Post, the arrangement is described as allowing “collection managers [to send] content tasking instructions directly to equipment installed at company-controlled locations,” rather than directly to company servers.

Government officials and the document itself made clear that the NSA regarded the identities of its private partners as PRISM’s most sensitive secret, fearing that the companies would withdraw from the program if exposed. “98 percent of PRISM production is based on Yahoo, Google and Microsoft; we need to make sure we don’t harm these sources,” the briefing’s author wrote in his speaker’s notes.

An internal presentation of 41 briefing slides on PRISM, dated April 2013 and intended for senior analysts in the NSA’s Signals Intelligence Directorate, described the new tool as the most prolific contributor to the President’s Daily Brief, which cited PRISM data in 1,477 items last year. According to the slides and other supporting materials obtained by The Post, “NSA reporting increasingly relies on PRISM” as its leading source of raw material, accounting for nearly 1 in 7 intelligence reports.

That is a remarkable figure in an agency that measures annual intake in the trillions of communications. It is all the more striking because the NSA, whose lawful mission is foreign intelligence, is reaching deep inside the machinery of American companies that host hundreds of millions of American-held accounts on American soil.

The technology companies, whose cooperation is essential to PRISM operations, include most of the dominant global players of Silicon Valley, according to the document. They are listed on a roster that bears their logos in order of entry into the program: “Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple.” PalTalk, although much smaller, has hosted traffic of substantial intelligence interest during the Arab Spring and in the ongoing Syrian civil war.

Dropbox, the cloud storage and synchronization service, is described as “coming soon.”

Sens. Ron Wyden (D-Ore.) and Mark Udall (D-Colo.), who had classified knowledge of the program as members of the Senate Intelligence Committee, were unable to speak of it when they warned in a Dec. 27, 2012, floor debate that the FISA Amendments Act had what both of them called a “back-door search loophole” for the content of innocent Americans who were swept up in a search for someone else.

“As it is written, there is nothing to prohibit the intelligence community from searching through a pile of communications, which may have been incidentally or accidentally been

collected without a warrant, to deliberately search for the phone calls or e-mails of specific Americans," Udall said.

Wyden repeatedly asked the NSA to estimate the number of Americans whose communications had been incidentally collected, and the agency's director, Lt. Gen. Keith B. Alexander, insisted there was no way to find out. Eventually Inspector General I. Charles McCullough III wrote Wyden a letter stating that it would violate the privacy of Americans in NSA data banks to try to estimate their number.

Roots in the '70s

PRISM is an heir, in one sense, to a history of intelligence alliances with as many as 100 trusted U.S. companies since the 1970s. The NSA calls these Special Source Operations, and PRISM falls under that rubric.

The Silicon Valley operation works alongside a parallel program, code-named BLARNEY, that gathers up "metadata" — technical information about communications traffic and network devices — as it streams past choke points along the backbone of the Internet. BLARNEY's top-secret program summary, set down in the slides alongside a cartoon insignia of a shamrock and a leprechaun hat, describes it as "an ongoing collection program that leverages IC [intelligence community] and commercial partnerships to gain access and exploit foreign intelligence obtained from global networks."

But the PRISM program appears to more nearly resemble the most controversial of the warrantless surveillance orders issued by President George W. Bush after the al-Qaeda attacks of Sept. 11, 2001. Its history, in which President Obama presided over exponential growth in a program that candidate Obama criticized, shows how fundamentally surveillance law and practice have shifted away from individual suspicion in favor of systematic, mass collection techniques.

The Obama administration points to ongoing safeguards in the form of "extensive procedures, specifically approved by the court, to ensure that only non-U.S. persons outside the U.S. are targeted, and that minimize the acquisition, retention and dissemination of incidentally acquired information about U.S. persons."

And it is true that the PRISM program is not a dragnet, exactly. From inside a company's data stream the NSA is capable of pulling out anything it likes, but under current rules the agency does not try to collect it all.

Analysts who use the system from a Web portal at Fort Meade, Md., key in "selectors," or search terms, that are designed to produce at least 51 percent confidence in a target's "foreignness." That is not a very stringent test. Training materials obtained by The Post instruct new analysts to make quarterly reports of any accidental collection of U.S. content, but add that "it's nothing to worry about."

Even when the system works just as advertised, with no American singled out for targeting, the NSA routinely collects a great deal of American content. That is described as "incidental," and it is inherent in contact chaining, one of the basic tools of the trade. To collect on a suspected spy or foreign terrorist means, at minimum, that everyone in the suspect's inbox or outbox is swept in. Intelligence analysts are typically taught to chain through contacts two "hops" out from their target, which increases "incidental collection" exponentially. The same math explains the aphorism, from the John Guare play, that no one is more than "six degrees of separation" from any other person.

A ‘directive’

In exchange for immunity from lawsuits, companies such as Yahoo and AOL are obliged to accept a “directive” from the attorney general and the director of national intelligence to open their servers to the FBI’s Data Intercept Technology Unit, which handles liaison to U.S. companies from the NSA. In 2008, Congress gave the Justice Department authority for a secret order from the Foreign Surveillance Intelligence Court to compel a reluctant company “to comply.”

In practice, there is room for a company to maneuver, delay or resist. When a clandestine intelligence program meets a highly regulated industry, said a lawyer with experience in bridging the gaps, neither side wants to risk a public fight. The engineering problems are so immense, in systems of such complexity and frequent change, that the FBI and NSA would be hard pressed to build in back doors without active help from each company.

Apple demonstrated that resistance is possible when it held out for more than five years, for reasons unknown, after Microsoft became PRISM’s first corporate partner in May 2007. Twitter, which has cultivated a reputation for aggressive defense of its users’ privacy, is still conspicuous by its absence from the list of “private sector partners.”

Google, like the other companies, denied that it permitted direct government access to its servers.

“Google cares deeply about the security of our users’ data,” a company spokesman said. “We disclose user data to government in accordance with the law, and we review all such requests carefully. From time to time, people allege that we have created a government ‘back door’ into our systems, but Google does not have a ‘back door’ for the government to access private user data.”

Microsoft also provided a statement: “We provide customer data only when we receive a legally binding order or subpoena to do so, and never on a voluntary basis. In addition we only ever comply with orders for requests about specific accounts or identifiers. If the government has a broader voluntary national security program to gather customer data we don’t participate in it.”

Yahoo also issued a denial.

“Yahoo! takes users’ privacy very seriously,” the company said in a statement. “We do not provide the government with direct access to our servers, systems, or network.”

Like market researchers, but with far more privileged access, collection managers in the NSA’s Special Source Operations group, which oversees the PRISM program, are drawn to the wealth of information about their subjects in online accounts. For much the same reason, civil libertarians and some ordinary users may be troubled by the menu available to analysts who hold the required clearances to “task” the PRISM system.

There has been “continued exponential growth in tasking to Facebook and Skype,” according to the PRISM slides. With a few clicks and an affirmation that the subject is believed to be engaged in terrorism, espionage or nuclear proliferation, an analyst obtains full access to Facebook’s “extensive search and surveillance capabilities against the variety of online social networking services.”

According to a separate “User’s Guide for PRISM Skype Collection,” that service can be monitored for audio when one end of the call is a conventional telephone and for any com-

bination of “audio, video, chat, and file transfers” when Skype users connect by computer alone. Google’s offerings include Gmail, voice and video chat, Google Drive files, photo libraries, and live surveillance of search terms.

Firsthand experience with these systems, and horror at their capabilities, is what drove a career intelligence officer to provide PowerPoint slides about PRISM and supporting materials to The Washington Post in order to expose what he believes to be a gross intrusion on privacy. “They quite literally can watch your ideas form as you type,” the officer said.

Poitras is a documentary filmmaker and MacArthur Fellow. Julie Tate, Robert O’Harrow Jr., Cecilia Kang and Ellen Nakashima contributed to this report.

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