

## Telefon- und Internetüberwachung

### Chronologie der Enthüllungen

Seit mehr als 2 Monaten nimmt der Skandal um die Internetüberwachung unter anderem durch US-amerikanische und europäische Geheimdienste einen zentralen Platz in den täglichen Nachrichten ein. Beinahe jeden Tag wird eine neue Enthüllung präsentiert und oft empören sich die selben sogleich über die NSA, die am nächsten Tag die Notwendigkeit vergleichbarer Überwachungsmaßnahmen in der EU, wie der Vorratsdatenspeicherung, unterstreichen. Die Fülle der Ereignisse und Berichte ist uns eine detaillierte Übersicht wert.

#### Juni 2013

**6. Juni 2013:** Die britische Zeitung *The Guardian* berichtet, dass der US-Geheimdienst NSA Telefondaten von Millionen US-EinwohnerInnen sammelt. Einem streng geheimen Gerichtsbeschluss zufolge müsse der Telefonanbieter Verizon Informationen wie Rufnummern, Standort und Dauer bezüglich aller Telefonate innerhalb der USA und von dort aus ins Ausland an den Geheimdienst weitergeben (Quelle: Heise, *The Guardian*).

**7. Juni 2013:** Die Berichte über die Spionageaktionen der US-Geheimdienste weiten sich aus. Laut dem *Wall Street Journal* sammelt die NSA neben den Telefondaten von Verizon auch jene der Kunden von AT&T und Sprint Nextel, sowie Metadaten über E-Mails, Internetsuchen und Kreditkartenzahlungen.

Der Guardian berichtet, dass NSA und FBI seit 2007 im Rahmen des streng geheimen Programms PRISM die zentralen Rechner von Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube und Apple anzapfen und damit Zugriff auf alle dort gesammelten Daten, wie Fotos, Emails, Dokumente oder Kontaktdaten erhalten. Dass dies mit ihrer Genehmigung erfolge, bestreiten die genannten Unternehmen. US-Präsident Barack Obama rechtfertigt die Telefon- und Internetüberwachung durch seine Regierung als Mittel zur Terrorismusbekämpfung.

Am selben Tag berichtet der Guardian, dass auch der britische Geheimdienst GCHQ seit 2010 von dem Netzspionage-Programm PRISM profitiere und insgesamt 197 Berichte auf Grundlage der so gewonnenen Daten erstellt habe. Diese könnten über ein gesondertes Programm abgegriffen werden, das speziell für den GCHQ eingerichtet worden sei. Wie lange und unter wessen Mitwisserschaft auf PRISM zugegriffen wurde, bleibe unklar (Quelle: *The Guardian*, Heise, *Wall Street Journal*).

**8. Juni 2013:** Der 29-jährige Techniker Edward Snowden bekennt sich in einem Videointerview mit dem Guardian öffentlich, die Quelle der Enthüllungen um das US-Spionageprogramm PRISM gewesen zu sein. Während die US-Regierung das ausufernde Sammeln von Daten leugnet und PRISM lediglich als ein internes Computersystem zur legalen Datensammlung darstellt, spricht Snowden, der als Mitarbeiter externer Unternehmen für den Geheimdienst tätig war, von einer „*infrastructure that allows it to intercept almost everything*“ (dt: „Infrastruktur, die es erlaubt, fast alles abzufangen“) (Quelle: *The Guardian*, Heise).

**12. Juni 2013:** Aus Kanada wird bekannt gegeben, dass dort ebenfalls seit Jahren eine massive Telefon- und Internetüberwa-

chung stattfindet. Der Verteidigungsminister Peter MacKay gibt zu, den Geheimdienst CSE zur weltweiten Ausspähung von Verbindungsdaten autorisiert zu haben (Quelle: Heise).

**13. Juni 2013:** Edward Snowden bringt einen neuen Aspekt in die Debatte um Hackerangriffe aus China gegen die USA, indem er berichtet, dass der US-Geheimdienst NSA China seit Jahren durch Hacker angreifen lasse. Seit 2009 habe es mehrere hundert Hackerangriffe auf China, weltweit mehr als 61.000 gegeben (Quelle: *The Guardian*, Heise).

**14. Juni 2013:** Die Finanznachrichtenagentur *Bloomberg* berichtet unter Bezugnahme auf nicht namentlich genannte InsiderInnen, dass die Zusammenarbeit zwischen Unternehmen und Geheimdiensten in den USA noch umfangreicher gewesen sei als bisher angenommen. Die Rede ist von tausenden Firmen, unter anderem Microsoft, die die Geheimdienste mit Informationen versorgt hätten. Dabei gehe es jedoch nicht um Kundendaten, sondern vor allem um Software-Schwachstellen, die das Hacken fremder Rechner erleichtern (Quelle: *Bloomberg*, Heise).

**16. Juni 2013:** Einem Bericht des *Spiegel* zufolge will der Bundesnachrichtendienst (BND) trotz des Skandals um PRISM & Co die Internetüberwachung wesentlich ausweiten. Mit einem 100 Millionen Euro teuren „Technikaufwuchsprogramm“ sollen sowohl der MitarbeiterInnenstab, als auch die technischen Möglichkeiten hierfür erweitert werden. 5 Millionen Euro seien bereits durch die Bundesregierung freigegeben worden.

Gleichzeitig spricht sich der Präsident des Bundeskriminalamtes (BKA) weiterhin vehement für die Vorratsdatenspeicherung, also die generelle, verdachtsunabhängige Speicherung von NutzerInnenendaten, aus (Quelle: *Spiegel*, Heise).

**19. Juni 2013:** Die *New York Times* rückt erneut die enge Verbindung zwischen US-Geheimdiensten und Internetunternehmen in den Fokus. So berichtet sie, dass Max Kelly, ehemals Sicherheitschef bei Facebook, inzwischen für die NSA arbeite. Weiter legt die Zeitung dar, dass Skype 2008 mit der Entwicklung eines geheimen Programms *Project Chess* begonnen habe, das den Sicherheitsbehörden den Zugang zu der Kommunikation der NutzerInnen erleichtern solle. Dies steht der Behauptung der in den PRISM-Skandal verwickelten Unternehmen entgegen, den Behörden sei kein direkter Zugriff auf ihre Server gewährt worden (Quelle: *New York Times*, Heise).

**20. Juni 2013:** Einem Bericht der *Times of India* zufolge, hat Indien im April 2013 ein *Central Monitoring System* (CMS) einge-

führt, das Sicherheits- und Steuerbehörden eine umfangreiche Überwachung von Internetkommunikation und Telefonanrufen ohne richterliche Genehmigung erlaubt.

Der *Guardian* veröffentlicht am gleichen Tag zwei streng geheime Dokumente, welche die Zielgruppe der Überwachungsprogramme in den USA konkretisieren. Danach könne eine Person, von der „vernünftigerweise“ angenommen werden kann, dass sie keine US-Staatsbürgerin ist und sich nicht in den USA aufhält, ohne richterliche Genehmigung von der NSA überwacht werden (Quelle: The Guardian, Heise).

**21. Juni 2013:** Edward Snowden gibt, wie der *Guardian* berichtet, belastende Informationen über den britischen Geheimdienst GCHQ preis. Dessen vor 18 Monaten in Betrieb genommenes Spionageprogramm *Tempora* sei sogar noch umfangreicher als PRISM. So fange der Geheimdienst in großem Stil Daten, wie E-Mails, Telefongespräche oder Einträge bei Facebook, über die transatlantischen Glasfaserkabel ab. Diese Daten würden auch der NSA zur Verfügung gestellt. In einem von Snowden überlassenen Dokument rühme sich der Geheimdienst damit, den „biggest internet access“ (dt.: umfassendsten Internet-Zugang) in einer Verbindung der Geheimdienste der USA, Großbritanniens, Kanadas, Neuseelands und Australiens unter dem Namen *Five Eyes* zu haben und „larger amounts of metadata than NSA“ (dt.: größere Mengen an Metadaten als die NSA) zu erfassen (Quelle: The Guardian, Heise).

**22. Juni 2013:** Die *New York Times* berichtet, dass von den USA am 14. Juni eine Anklage gegen Edward Snowden wegen Spionage und Diebstahl von Regierungseigentum beim Bundesgericht in Virginia eingereicht worden sei. Snowden hält sich zu diesem Zeitpunkt in Hongkong auf (Quelle: New York Times, Heise).

**23. Juni 2013:** Edward Snowden berichtet in einem Interview mit der *South China Morning Post*, dass die NSA in China Millionen Mobilfunknachrichten abgehört und Datenübertragungsleitung der Pekinger Tsinghua-Universität überwacht habe. Weiter habe es Snowden zufolge 2009 Angriffe auf Computer von Pacnet, Betreiber eines der größten Glasfasernetze in der Asien-Pazifik-Region und verantwortlich für den Internetverkehr mit den USA, gegeben. Diese seien jedoch wieder eingestellt worden (Quelle: Heise).

**24. Juni 2013:** Die *Süddeutsche Zeitung* berichtet, dass im Rahmen des britischen Überwachungs-Programms *Tempora* auch das Glasfaserkabel TAT-14 ausgespäht worden sei, über das ein beträchtlicher Teil der Übersee-Kommunikation aus Deutschland laufe. Entsprechend sei auch der deutsche Telefon- und Internetverkehr Gegenstand der Überwachung gewesen. Die Bundesregierung und der Bundesnachrichtendienst (BND) bestreiten, darüber Kenntnis gehabt zu haben (Quelle: Süddeutsche Zeitung, Heise).

**30. Juni 2013:** Aus neu ausgewerteten NSA-Dokumenten geht dem *Spiegel* zufolge hervor, dass die Bundesrepublik in besonderem Maße von den US-Geheimdiensten überwacht wurde. Rund eine halbe Million Kommunikationsverbindungen seien betroffen. Auch die EU sei den Dokumenten zufolge Ziel der Spionageattacken geworden. In einem anderen Dokument, das

dem *Guardian* vorliegt, werden 38 Botschaften und diplomatische Vertretungen aufgeführt, die von der massiven Ausspähung durch den US-Geheimdienst betroffen seien, unter ihnen auch die Botschaften Frankreichs, Italiens, Griechenlands, sowie Japans, Mexikos, Südkoreas, Indiens und der Türkei.

Die *Washington Post* veröffentlicht unterdessen neue Folien zum US-Überwachungsprogramm PRISM, aus denen hervorgeht, dass Daten von Microsoft, Google, Facebook, Youtube, Skype und anderen nicht einfach abgefragt, sondern in Echtzeit überwacht wurden. Mit einer beim Diensteanbieter installierten Filtersoftware seien Daten nach Schlüsselwörtern durchsucht worden, um die Datenströme auszudünnen (Quelle: Der Spiegel, Heise, The Guardian, Washington Post).

## Juli 2013

**2. Juli 2013:** Wie Experten aus dem Umfeld des deutschen Internet-Knotens De-CIX in Frankfurt am Main gegenüber *heise online* bestätigten, wird ein nicht näher definierter Teil der über den Knoten laufenden Daten an den BND und andere „Bedarfsträger“ übermittelt. Dem Vorsitzenden der G10-Kommission Hans De With zufolge, der die Abhörtätigkeit wie auch die Justizministerin Sabine Leutheusser-Schnarrenberger bestätigte, bestünde eine Obergrenze von 20 Prozent des Datenverkehrs (Quelle: Heise).

**3. Juli 2013:** Über einen Bericht der *New York Times* wird bekannt, dass die US-Geheimdienste den gesamten Briefverkehr innerhalb des Landes registrieren lassen. Im Rahmen des Programms *Mail Isolation Control and Tracking* wurden den InformantInnen aus Justizministerium und FBI zufolge AbsenderInnen und EmpfängerInnen von rund 160 Milliarden Postsendungen abfotografiert und gespeichert (Quelle: New York Times, Heise).

**4. Juli 2013:** Wie die Tageszeitung *Le Monde* berichtet, überwacht und speichert der französische Auslandsnachrichtendienst *Direction Générale de la Sécurité Extérieure* (DGSE) die Kommunikation der französischen StaatsbürgerInnen seit Jahren. Zu den gespeicherten Daten, die bei Bedarf an andere Behörden weitergeleitet würden, gehörten die Metadaten aller Telefongespräche, E-Mails, SMS, sämtliche Aktivitäten bei Google, Facebook, Microsoft, Apple oder Yahoo (Quelle: Heise).

**6. Juli 2013:** Die *New York Times* berichtet von einer erheblichen Erweiterung der NSA-Befugnisse durch den *Foreign Intelligence Surveillance Court* (FISC). In geheimen Urteilen sei der NSA unter anderem gestattet worden, Daten etwa bei Verdacht auf einen Zusammenhang mit Cyberangriffen oder dem iranischen Atomwaffenprogramm auch ohne richterliche Genehmigung auszuspähen (Quelle: Heise, New York Times, Süddeutsche Zeitung).

**7. Juli 2013:** Einem Bericht der brasilianischen Zeitung *O Globo* zufolge wurden auch brasilianische BürgerInnen konstant durch die NSA überwacht. E-Mails und Telefongespräche seien hier in noch größerem Ausmaß abgefangen worden als in anderen lateinamerikanischen Ländern. Der Zeitung vorliegenden Dokumenten zufolge seien die Daten mit Hilfe des Programms *Fairview* ausgespäht worden, das gemeinsam mit einer großen US-Telekom-

munikationsfirma genutzt werde. Partnerschaften des Unternehmens mit anderen Firmen der Telekom-Branche, unter anderem in Brasilien, ermöglichten es der NSA schließlich auf die Daten in verschiedenen Ländern der Welt zuzugreifen. Inwieweit die Telekom-Firmen darüber informiert sind, sei nicht bekannt.

Der *Spiegel* veröffentlicht ein Interview mit Edward Snowden, in dem dieser erklärt, dass der BND und andere ausländische Geheimdienste, ebenso wie verschiedene Telekom-Firmen, eng mit der NSA zusammenarbeiten. So habe die NSA dem BND etwa Analyse-Werkzeuge zur Verfügung gestellt, mit denen der BND Datenströme aus fünf digitalen Knotenpunkten anzapfe und an die Zentrale in Pullach weiterleite. Ob auch die NSA selbst Internetknotenpunkte in Deutschland ausspioniere, sei nicht geklärt. Weiter ist die Rede von einem geheimen NSA-Abhörzentrum namens *Consolidated Intelligence Center* in Wiesbaden, dessen Neubau durch den BND genehmigt worden sei.

Nach dem Bekanntwerden der Post-Überwachung in den USA, räumt auch die deutsche Post auf einen entsprechenden Tweet des CCC-Sprechers Frank Rieger hin ein, Adressdaten auf Briefen und Paketen automatisch zu scannen und zu speichern (Quelle: Heise, Spiegel).

**9. Juli 2013:** Anlässlich mehrerer Klagen vor dem EuGH gegen die Vorratsdatenspeicherung verteidigten VertreterInnen der EU-Gremien und -Mitgliedsstaaten die Richtlinie zur verdachtsunabhängigen Speicherung aller Verbindungsdaten in einer Anhörung.

Das Urteil zu dem nun beendeten Verfahren wird in etwa sechs Monaten erwartet. Das Gutachten des Generalanwalts soll am 9. November 2013 veröffentlicht werden (Quelle: Heise, Netzpolitik.org).

**12. Juli 2013:** Einem Bericht des *Guardian* zufolge hat Microsoft die NSA darin unterstützt, auch verschlüsselte NutzerInnen-Daten auszuspähen. So sei etwa vor dem Start des Mail-Portals Outlook.com sichergestellt worden, dass die NSA auf Daten zugreifen könne, bevor sie verschlüsselt werden. Auch an der Erleichterung des Zugangs zu Daten in dem Online-Speicherdienst SkyDrive und der Kommunikation via Skype sei gemeinsam gearbeitet worden (Quelle: The Guardian, Heise).

**15. Juli 2013:** Nachdem bereits in der vergangenen Woche Edward Snowden im *Spiegel* von einer umfangreichen Zusammenarbeit zwischen NSA und BND berichtet hatte, schaltet sich nun auch die *Bild* in die Debatte ein, die anführt, aus US-Regierungskreisen weitere Details dieser Zusammenarbeit erfahren zu haben. Der BND habe über Jahre von der umfangreichen Überwachung durch die NSA profitiert, etwa im Falle einer Entführung deutscher StaatsbürgerInnen. Es sei, so folgert die Zeitung, daher nur naheliegend, dass er über die umfangreiche

Überwachung und Datensammlung durch den US-amerikanischen Geheimdienst informiert gewesen sei. Auch zieht die *Bild* die Behauptung des jüngst von einer umstrittenen USA-Reise zurückgekehrten Bundesinnenministers Hans-Peter Friedrich in Zweifel, dass die Überwachungsprogramme Daten gezielt nach Inhalten scannen würden – die Kommunikation würde vielmehr flächendeckend gespeichert (Quelle: Heise, Bild.de).

**17. Juli 2013:** Auch die Bundeswehr arbeite, so die *Bild*, mit der NSA zusammen. Einem geheimen Nato-Dokument zu Folge sei sie seit Herbst 2011 über PRISM informiert. Die Vorwürfe würden durch das Auftauchen einer zweiten Datenbank mit dem Namen PRISM erhärtet, die im Kommandobereich der Bundeswehr in Afghanistan zur Überwachung von Terrorverdächtigen genutzt worden sei. Ein Zusammenhang zwischen den beiden Programmen weisen SprecherInnen der Bundesregierung und des BND zurück. Bei PRISM II handele es sich um ein nicht geheimes Isaf-Programm zur Radaraufklärung und Luftüberwachung. Dies steht Berichten der *Bild* entgegen, denen zufolge beide Programme auf dieselben NSA-Datenbanken zugreifen würden.

Das ARD Magazin FAKT berichtet, dass es sich bei der vom BND verwendeten Software der Boeing-Tochter Naurus um PRISM-Software handele (Quelle: Heise, Bild.de).

**18. Juli 2013:** Die *Mitteldeutsche Zeitung Halle* berichtet, dass in Wiesbaden-Erbenheim aktuell ein Zentrum für militärische Aufklärung, *Consolidated Intelligence Center*, durch die amerikanischen Streitkräfte gebaut wird. Der Zeitung zufolge handelt es sich dabei um ein Abhörzentrum der NSA (Quelle: Heise).

**20. Juli 2013:** Wie der *Spiegel* berichtet, nutzen deutsche Geheimdienste die Ausspähdatenbanken der NSA stärker als sie zugeben wollen. Geheimen Unterlagen zufolge setzten BND und BfV eine NSA-Software namens *XKeyscore* ein, die quasi eine „digitale Totalüberwachung“ ermögliche. Von dem Programm sei ein Teil der monatlich bis zu 500 Millionen Datensätze aus Deutschland, unter anderem Telefonnummern, E-Mail-Adressen und Zeitstempel von Nutzeraktivitäten, erfasst, auf die auch die NSA Zugriff habe.

In den USA wird die die Genehmigung zum Sammeln von Telefonverbindungsdaten durch die US-Behörden derweil verlängert (Quelle: Heise, Spiegel).

**26. Juli 2013:** Die Gewerkschaft der Polizei spricht sich trotz der jüngsten Überwachungsskandale für die Vorratsdatenspeicherung aus.

US-Medien berichten, dass Regierungsbehörden von Dienstbietern im Internet die Herausgabe der geheimen Schlüssel ihrer

Sara Stadler

Sara Stadler studierte Informatik an der Hochschule Bremen und arbeitete in der FfF-Geschäftsstelle.

Server mit SSL-Verschlüsselung verlangten. Die Konzerne würden die Herausgabe der *Master-Keys*, mit denen die gesamte Kommunikation des Servers auch im Nachhinein entschlüsselt werden könnte, jedoch bislang verweigern (Quelle: Heise).

**27. Juli 2013:** Der frühere Bundesinnenminister Otto Schily (SPD) räumt in einem Interview mit dem *Spiegel* ein, dass PRISM im Grunde nichts anderes sei als die Vorratsdatenspeicherung (Quelle: Spiegel).

**31. Juli 2013:** Der *Guardian* veröffentlicht weitere Details zum NSA-Programm *XKeyscore*. Folien aus dem Fundus Edward Snowdens zufolge ermögliche das Programm eine nahezu vollständige Überwachung der Internetnutzung (E-Mails, Chats, Browser-Chroniken, Aktivitäten auf Facebook) sowie die Möglichkeit einer vollständigen Überwachung jeder beliebigen Person bis hin zum US-Präsidenten (Quelle: Heise, The Guardian, Spiegel).

## August 2013

**1. August 2013:** Unter Berufung auf weitere, von Edward Snowden ausgehende Dokumente berichtet der *Guardian* von einer umfangreichen Finanzierung des britischen Geheimdienstes GCHQ durch die NSA. Mindestens 100 Millionen Pfund seien in der vergangenen drei Jahren geflossen. Dass dafür auch US-BürgerInnen vom GCHQ überwacht worden seien, weise die NSA zurück. Weitere aus den Dokumenten gewonnene Erkenntnisse beziehen sich auf die Telefonüberwachung, in die der GCHQ massiv investiert habe, sowie den GCHQ-Standort in der Küstenstadt Bude, an dem der Geheimdienst Berichten der *Süddeutschen Zeitung* und des *NDR* zufolge Daten aus dem Glasfaserkabel TAT-14 abgefangen habe. Für die Sanierung dieses Standortes habe Großbritannien 15,5 Millionen Pfund von der NSA erhalten (Quelle: Heise, The Guardian).

**2. August 2013:** Die *Süddeutsche Zeitung* und der *NDR* veröffentlichten die Namen derjenigen Telekom-Firmen, die dem britischen Nachrichtendienst GCHQ bei der Internetüberwachung behilflich waren. Genannt werden unter anderem die international tätigen Unternehmen British Telecom, Verizon und Vodafone.

Aus Neuseeland werden einstweilen Pläne bekannt, die Befugnisse des Geheimdienstes GSCB auszuweiten und den bestehenden Apparat zur Überwachung von Telefon und Internetkommunikation fortan auch für die Überwachung von StaatsbürgerInnen und Personen mit einem dauerhaften Aufenthaltsstatus zu nutzen (Quelle: Süddeutsche Zeitung, NDR, Heise).

**3. August 2013:** *CNET News* berichtet, dass die US-Regierung und das FBI NetzbetreiberInnen zur Installation von Port Readern zwingen (Quelle: Heise, CNET).

**4. August 2013:** Aus einem Bericht des *Spiegel* geht hervor, dass der BND Daten aus der eigenen Fernmeldeaufklärung an die NSA übermittele. Hinter einer der Datensammelstellen, über

die die NSA im Dezember vergangenen Jahres rund 500 Millionen Metadaten aus der Bundesrepublik erfasst habe, verberge sich möglicherweise der BND-Standort Bad Aibling. Auch ansonsten sei die Zusammenarbeit zwischen BND und NSA enger als bisher angenommen. Die Zeitschrift berichtet von Schulungen – unter anderem im Umgang mit dem Programm *XKeyscore* – die VertreterInnen des BND und des Bundesamtes für Verfassungsschutz von NSA-SpezialistInnen erhalten hätten (Quelle: Heise, Spiegel).

**5. August 2013:** Die *New York Times* berichtet, dass die NSA Informationen an Ermittlungsbehörden weiterleite, obwohl deren Einsatz gegen in den USA lebende StaatsbürgerInnen nicht ohne weiteres möglich sein sollte (Quelle: Heise, New York Times).

**7. August 2013:** Der ehemalige NSA-Direktor Michael Hayden bestätigt in einem Interview mit CNN alle aus den von Snowden veröffentlichten Folien hervorgehenden Daten über das Programm *XKeyscore* und bewertet diese als positive Errungenschaft.

Die *Tagesschau* berichtet einstweilen unter Berufung auf den stellvertretenden Sprecher der Bundesregierung Georg Streiter, dass die Zusammenarbeit zwischen BND und NSA im April 2002 von der rot-grünen Bundesregierung vertraglich festgelegt und von dem damaligen Kanzleramtsminister Frank-Walter Steinmeier (SPD) absegnet worden sei (Quelle: Heise, Tagesschau.de).

**8. August 2013:** Die EU-Kommission legt ein Papier zum *Nachweis der Erforderlichkeit der Vorratsdatenspeicherung* vor.

Die *New York Times* fördert unterdessen neue Informationen über das Ausmaß der Online-Überwachung in den USA durch die NSA zutage. So sei nicht, wie von offizieller Seite stets betont wurde, „lediglich“ die Kommunikation mit nicht-US-BürgerInnen ohne Genehmigung überwacht, sondern jegliche Kommunikation nach Verweisen auf überwachte Personen gescannt worden (Quelle: Heise, New York Times).

**9. August 2013:** Die US-amerikanischen E-Mail-Anbieter *Lavabit* und *Silent Circle* machen dicht. Beide hatten ihren NutzerInnen verschlüsselte Kommunikation angeboten. Auch wenn die Anbieter die Gründe für das Aus nicht nennen (dürfen), legen die Aussagen des Lavabit-Chefs Ladar Levison nahe, dass sie, zumindest in diesem Fall, etwas mit der Weigerung zu tun hatten, den US-Behörden Zugriff auf Kommunikationsdaten zu ermöglichen (Quelle: Heise).

**16. August 2013:** Nach Berichten der *Washington Post* hat die NSA entgegen anderslautender Beteuerungen in erheblichem Umfang illegal US-BürgerInnen überwacht. Ein geheimer Bericht, der den Großraum Washington D.C. abdeckt, berichte von 2776 „Vorfällen“ über einen Zeitraum von 12 Monaten. Nach Angaben der NSA sei die Überwachung „versehentlich“ aufgrund eines Programmierfehlers erfolgt. Offenbar wurde bei der Telefonüberwachung die Vorwahl von Washington D.C. (202) mit der Ländervorwahl von Ägypten (20) verwechselt (Quelle: Washington Post, Spiegel).

