Was ist neu an PRISM & Tempora?
Denkanstöße zur Überwachung der Menschen durch Geheimdienste

Inhaltsverzeichnis

Einleitung....3
Post-Privacy contra Datenschutz....3
Was ist neu an PRISM und Tempora?....4
Was ist erlaubt - was nicht?....4
Wie ist diese Überwachungspraxis in den USA entstanden?....5
Ist das alles neu?....6
Was sagen die US-Bürger dazu?....6
Gefahren auch ohne Geheimdienste (nicht vergessen!)....7
Ich habe doch nichts zu verbergen!....8
Der Dampfdruckkochtopf oder was sind die 15000 "bösen Worte"....9
Wie kann man sich schützen?....9
Forderungen an Wirtschaft und Staat....10

Einleitung

Diese Publikation ist auch nach 8 Jahren noch in Arbeit, denn ständig werden mehr Details unserer Überwachung aufgedeckt ….

Am 23. August 2013 war die Arbeitsgruppe Polizei&Geheimdienste von Aktion Freiheit statt Angst eingeladen einen Workshop zu PRISM & Tempora abzuhalten. Wir möchten hier unsere Eingangsstatements, aber vor allem die Ergebnisse der Diskussion darstellen, denn bisher haben wir in den letzten 3 Monaten fast 50 Artikel aus Zeitschriften zu diesem Themenkomplex in unserem Web zitiert, es fehlte aber eine eigene Einschätzung und Einordnung dieses Skandals.

Post-Privacy contra Datenschutz

Wenn ich alles offen ins Netz stelle, kann/braucht mich keiner überwachen. Mit dieser irrigen These überdecken viele oft junge Menschen die Beklemmungen, die einen mit jeder neuen Veröffentlichung mehr beschleichen.

Der Chaos Computer Club hat dagegen gesetzt: **Persönliche Daten schützen - Öffentliche Daten nützen!**

Datenschutz ist nicht alles - Informationsfreiheit gehört dazu!

Diese bezieht sich aber auf das Wissen über Vorgänge in Staat und Wirtschaft. Die Privatsphäre des Einzelnen ist dagegen ein fundamentales Grundrecht - rechtlich spätestens seit dem Volkszählungsurteil von 1983.

Die 1. Folgerung daraus lautet:
Datenschutz und Informationsfreiheit gehören zusammen. Whistleblowing ist eine notwendige Konsequenz solange uns Staat und Wirtschaft nicht ungehinderten Zugang zu ihren Daten liefern.

Whistleblower müssen geschützt werden - ein Gesetz dazu fehlt bislang.

Unsere Forderung: Asyl für Edward Snwoden und Bradley Manning

Was ist neu an PRISM und Tempora?

Die Zeitungen sprechen von vollständiger Überwachung aller Menschen (zumindest in Europa und wohl auch anderswo).

Siehe dazu

- Mutti, komplett heißt auch komplett
- Bundesregierung für "alles speichern"
- Eine Million voll oder alle ein wenig
- Zugriff auf alles durch "XKeyscore"?
- Ein Verdächtiger - Millionen Überwachte

Unsere Bundeskanzlerin ist da anderer Meinung. Mutti stellt zu PRISM&Tempora fest, dass nur 1% der Kommunikationsdaten in Deutschland durch ausländische Dienste abgefangen wird. Das sind zwar immerhin 500 Mio. Verbindungen/Mon. aber "*man könne nicht von vollständiger Überwachung sprechen*".

Was ihr selbst Sorge macht, worüber aber niemand in der Regierung redet, ist das Thema Wirtschaftsspionage, denn in dem 1% sind auch massig Daten aus dem Geschäftsverkehr enthalten. Welche Folgen das für den Wirtschaftsstandort Deutschland seit Jahren hat wird wohl geheim bleiben (s. dazu z.B. Wirtschaftsspionage kostet uns 50 Milliarden).

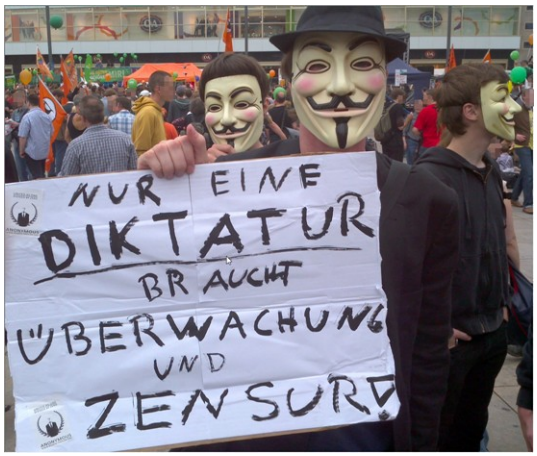
Die 2. Folgerung lautet also: Nicht alle 82 Millionen werden vollständig überwacht aber zumindest jeder ein bisschen, statistisch gesehen, Jede/r ca. 6-mal im Monat.

Was ist erlaubt - was nicht?

Konservative Zeitungen wimmeln ab: Geheimdienste gab es schon immer und die sind auch "nur nach ihren Gesetzen tätig".

Das stimmt nicht! Die jetzt aufgedeckte Praxis ist das Gegenteil von gesetzestreu. Jeder (Auslands-) Geheimdienst darf im Ausland tätig werden, Grenzen setzt man sich lediglich durch die Menschenrechte (außer man will mal gerade ein paar Terroristen töten). Einschränkungen gibt es (aber nur manchmal) beim Einsatz gegen eigene Bürger im Ausland.

Während die Überwachung durch die Polizei nach Gesetzen und bekannten Paragrafen und in der Regel mit einem Richtervorbehalt geschieht, läuft die Überwachung durch Geheimdienste z.B. in Deutschland nach dem G-10 Gesetz von 1968 und nur ein Kontrollausschuss kann in die Arbeit der Geheimdienste, natürlich streng vertraulich, Einsicht nehmen.



Fazit: Die NSA darf in Deutschland spionieren und der BND in den USA und dann tauscht man freundschaftlich die Ergebnisse aus und kein Gesetz wurde formal verletzt.

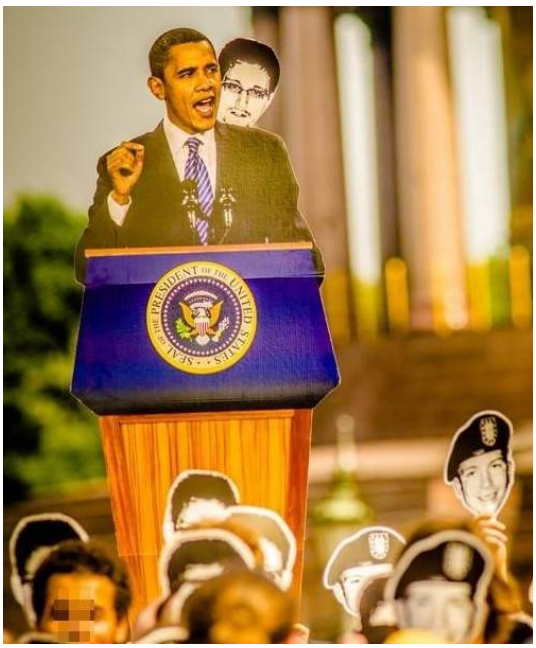
Das wäre schon schlimm genug aber die Washington Post berichtet von 1200 Übertretungen der eigenen Regeln durch die NSA pro Jahr. Eine Zahl für unsere Geheimdienste ist nicht bekannt, aber es gibt Fälle, die schlimmes befürchten lassen:

- Verfassungsschutz belog Journalistin
- Verfassungsschutz für 40 Jahre Überwachung verurteilt
- Journalist überwacht wegen US-Kritik?

Die 3. Folgerung: Die Enthüllungen von Edward Snowden bringen so etwas wie das Tschernobyl des Datenschutzes ans Tageslicht.

Wie ist diese Überwachungspraxis in den USA entstanden?

Lassen wir die ebenso ungesetzliche Gesinnungsschnüffelei eines FBI Chefs Hoover in den 50-er Jahren mal beiseite, Dann basieren die Überwachungsprogramme der NSA mehrheitlich auf Regelungen von US-Präsident Ronald Reagan aus dem Jahr 1981. Das belegen bislang geheimen Akten, deren Herausgabe die American Civil Liberties Union (ACLU) und die MFIA der Yale Law School erreicht haben. Dass Reagans präsidiales Dekret 12333 eine juristische Säule der Überwachung ist, war bekannt, aber im Zuge des NSA-Skandals war ihm bislang die mit Abstand geringste Aufmerksamkeit zuteil geworden. Dabei heißt es in einem NSA-Memo vom 19. Juni 2013 – also nach Beginn der Snowden-Enthüllungen: "Die NSA unternimmt die Mehrzahl ihrer Überwachungsaktivitäten ausschließlich unter den Befugnissen des Dekrets 12333."



Dieses Dekret erlaubt die Überwachung von Handys und Smartphones in aller Welt, aber auch den Angriff auf interne Leitungen von Google und Yahoo sowie die Sammlung von Millionen Adressbüchern und die komplette Telefonüberwachung in mindestens zwei US-Staaten. Im Gegensatz zu Abschnitt 215 des Patriot Acts und Abschnitt 702 des FISA Amendment Acts weist das Dekret aber einen ganz entscheidenden Unterschied auf. Da das Dekret 12333 direkt vom US-Präsidenten stammt und auch von der Exekutive implementiert wurde, gebe es so gut wie keine Kontrolle durch das Parlament oder die Gerichte, schreibt die ACLU.

Neu ist auch, dass durch das Dekret der Begriff der "Datensammlung" verschleiert wird, da eine "Datensammlung" die Entgegennahme durch eine Person erfordert. Eine automatische Sammlung (gathering) ist damit keine "Datensammlung".

Dokumente, die für Diskussionen sorgen werden sich auch die 16 Ausnahmen, in denen die Defense Intelligence Agency sogar US-Personen überwachen darf. Eigentlich sollten die in den USA vor Überwachung geschützt sein.

Somit bewahrheitet sich die Aussage von John Napier Tye, einem ehemaligen Mitarbeiter des US-Außenministeriums. Der hatte Ende Juli 2014 erklärt, das Dekret 12333 müsse als Grundlage für die weltweite Überwachung herhalten und unterliege keinerlei demokratischer oder juristischer Kontrolle. (s. http://www.heise.de/newsticker/meldung/Geheimgesetz-NSA-Ueberwachung-basiert-auf-Reagan-Dekret-2405517.html).

Ist das alles neu?

Prof. Foschepoth hat in seinem Buch "Post- u. Telefonüberwachung in der BRD" bereits im letzten Jahr darüber geschrieben, dass die Überwachung von Post und Telefon zuerst durch die Westalliierten und ab Mitte der 50-er Jahre durch deutsche Geheimdienste dem Treiben der DDR-Kollegen in nichts nachstand. Heute stehen bei jedem größeren Provider an den Routern die sogenannten SINA Boxen, mit denen sich die Geheimdienste Zugang zum durchlaufenden Datenverkehr verschaffen können. Die Atlantikkabel wurden auch schon im 1. Weltkrieg angezapft.

Wir dürfen nicht vergessen, dass das Internet aus der Küche des US Verteidigungsministeriums aus dem DARPA-Netz entstanden ist. Die Struktur und der Aufbau des Internets wird noch immer von den USA dominiert. Von den 12 Root-Domain-Name Servern (DNS) stehen 6 in USA, 2 in der EU und 2 in Asien. Das ICANN, die Domain-Namen-Vergabe-Organisation führt gerade eine Vorratsdatenspeicherung (VDS) für Domain-Inhaber ein.

Siehe dazu

- ICANN als Erfüllungsgehilfe der Staaten?
- USA wollen dauerhafte Kontrolle über Internet-Verwaltung
- Überwachtes Deutschland

Was sagen die US-Bürger dazu?

Der deutsche oder europäische Datenschutz ist in den USA unbekannt. Privacy bietet nach US-Recht nur Schutz gegen den Staat und nur für die eigenen Bürger. Die Wirtschaft kann dort mit den Daten der Bürger tun was sie in den AGBs definiert.

Zusätzlich sind die großen Dienstanbieter und Softwareproduzenten in den USA, wie Google, Apple, Microsoft, Facebook, Youtube, ... verpflichtet Daten ausländischer Bürger an interessierte staatliche Stellen weiterzuleiten. Zunehmend erkennen inzwischen auch die US-Bürger, dass diese Weitergabe es oft mit dem Wohnsitz der Betreffenden nicht so genau genommen hat.

Interessant ist in diesem Zusammenhang, dass auch in den USA nicht der große Aufschrei der Empörung ausbricht und die "Dienste" sich bescheiden in irgendwelche Kämmerchen zurückziehen, sondern, dass nach den Enthüllungen sogar noch Druck gegen Provider aufgebaut wurde, die den "Densten" durch das Angebot von Verschlüsselung von E-Mail, Chat oder Telefon das Leben schwer gemacht hatten. Zwei größere E-Mail-Anbieter haben daraufhin ihr Angebot eingestellt, um nicht zur Herausgabe ihrer Kundendaten gezwungen zu werden.

In einem WDR Bericht über den arabischen Frühling wurde die Ex-Außenministerin Hillary Clinton zitiert, dass sich die USA für Anonymität im Datenverkehr in Diktaturen einsetzen und an einigen US-Universitäten Proxy-Server vorhalten, die den dortigen Dissidenten ein Sprachrohr verleihen soll. Im eigenen Land darf es dagegen scheinbar keine Anonymität geben.

Dafür haben die US-Geheimdienste "nette" Programme im Einsatz, um durch eine steuernde Person 32 "Echte" fiktive Persönlichkeiten in sozialen Netzwerken zu erschaffen, die dann mit diesen gefälschte Internet-Identitäten in Online-Diensten und Social Media Plattformen interagieren - natürlich nur um Terroristen zu entlarven (oder erst zu erzeugen).

Nebeneffekt: Das führt dann auch mal dazu, dass die Geheimdienste Geld verschwenden, um sich gegenseitig ihre "erfundenen Organisationen" überwachen, siehe z.B.

- Wenn die einen Hand nicht weiß, was die andere tut
- Ein englischer Spitzel soll die Demonstranten in Heiligendamm unterwandern
- US Geheimdienste gegen HADOPI
- Paralleluniversum oder Methode?

Gefahren auch ohne Geheimdienste (nicht vergessen!)

Schieben wir nicht alles auf die "bösen Geheimdienste" - die werden sich nicht wehren sondern in ihrem Image sonnen. Für den Datenklau bei und durch Facebook u.a. ist das Wirtschaftsmodell verantwortlich. Wir zahlen mit unseren Daten und ordnen uns jeder noch so unrechtmäßigen Änderung der AGBs unter anstatt solche Unternehmen durch Nichtnutzung zu strafen.

Es gibt Zensur bei Facebook - das ist kein **soziales** Netzwerk. Die Facebook Seiten von OpenBook, einem Protestprojekt gegen Facebook, wurden gelöscht. UK Uncut war eine regierungskritische Gruppe in Großbritannien, deren Seiten ebenfalls gelöscht wurden. Auch wir kennen Beispiele, wo Beiträge von Kollegen entfernt wurden. Es gibt auch keinen Grund in diesem a- sozialem Netzwerk zu sein, denn für etwas Geld werden dort auch einfach Geschichten erfunden (s. "Sponsored Stories" sind Facebooks neuer Werbetrick).

Auf 88% aller Domains im Internet sind Web-Bugs von Google versteckt, das sind 1x1 Pixel große unsichtbare Bilder, die nur dazu dienen "nach Hause zu telefonieren". Das dient natürlich "nur statistischen Zwecken" - und alle machen mit.

Die Verschlüsselung im deutschen DE-Mail-Dienst ist unsicher, jeder weiß das und trotzdem spricht die Bundesregierung dabei von Innovation.

Siehe

- De-Mail wegen PRISM & Co. ein Lacher
- Elektronischer Personalausweis und das Bürgerportal
- Deutsche Post steigt bei De-Mail aus
- CCC kritisiert weiterhin DE-Mail

Der Landtag von NRW betreibt seinen Mail-Server in den USA. Spionage war noch nie so einfach wie heute. (s. NRW Minister können abgehört werden

Ich habe doch nichts zu verbergen!

Jeder kennt den Spruch: **Ich habe doch nichts zu verbergen.**

Doch, jede/r hat was zu verbergen, denn es geht um das eigene Leben oder sogar Überleben.

Einige wenige Beispiele dazu:

- Justin Carter, 18 Jahre, chattet mit den Bemerkungen LoL und just kidding, er will seine Mitschüler umbringen. Nun sitzt er seit Jahresanfang im US-Knast und ihm drohen als "Terrorist" 8 Jahre (Bei Facebook-Spruch 8 Jahre Knast)
- Ein CDU Student befragt für seine Islam-Magisterarbeit auch einen beobachteten "Islamisten" und bekommt Schwierigkeiten bei der Einstellung in den öffentlichen Dienst in Baden-Württemberg.
- Immer mehr Menschen laufen bei uns mit der elektronischen Gesundheitskarte (eGK), dem ePerso herum und können an jedem Ort gescannt und identifiziert werden. (s. Elektronischer Personalausweis und das Bürgerportal oder Definition RFID)
- Andere benutzen die unsichere DE-Mail und verlassen sich auf die Versicherung "das ist rechtssicher und verschlüsselt". (Links s. oben)
- In Hamburg bekommen Schüler ihr Schulessen nur gegen Fingerabdruck. Was könnte der Kantinenbetreiber mit den Daten über Essgewohnheiten und dem Fingerabdruck machen? (s. Essen nur gegen Fingerabdruck)
- Alle kennen die Datenpannen bei Telekom, Bahn und Versicherungen, wo unsere persönlichen Gewohnheiten plötzlich zur Ware werden. (s. T-Datenskandal - Zumwinkel attackiert Telekomchef Obermann)
- Das Grazer Büro eines Autozulieferers schickt einen Kfz-Techniker auf Dienstreise in die USA. Der Mann wird bei Ankunft 2 Tage und Nächte in einem dunklen Keller verhört und dann ohne Begründung wieder ins Flugzeug nach Hause gesetzt.
- Bei einer Veranstaltung zur Speicherung von Flugreisedaten in der Berliner C-Base berichtet eine Frau, dass sie mit ihrem Freund von Düsseldorf nach Puerto Rico fliegen will. Beim Einchecken wird dem Mann ohne Begründung ein Mitflug verweigert. Die Fluggesellschaft weiß nichts, die Bundespolizei auch nicht. Urlaub im Eimer durch die No-Fly-Liste - das ist absolute Rechtlosigkeit.
- Ein Exil-Syrer, der in Kanada lebt will von Toronto über New York nach Europa fliegen. In New York wird er im Transitbereich festgenommen und nach Syrien zum Foltern gebracht. Er sitzt noch immer dort im Kerker.
- Der Internetaktivist Jakob Appelbaum wohnt jetzt in Deutschland, nachdem er und seine Partnerin mehrfach von US-Diensten verhört wurden. (s. "Überwachung hat die Macht, Menschen zu ermorden")

Dazu gibt es ein **schönes Lied**: Nichts zu verbergen - *Nothing to hide - Rien a cacher*
Text in französisch und englisch http://www.laparisienneliberee.com/rien-a-cacher/
Video in französisch

Der Dampfdruckkochtopf oder was sind die 15000 "bösen Worte"

… und was bleibt von der Sprache wenn man sie meidet?

Eine britische Zeitung hat die 15.000 Worte aufgelistet, bei deren Erscheinen in E-Mail oder am Telefon die Programme der Geheimdienste Alarm schlagen. Der normale Wortschatz in der Umgangssprache liegt bei 5000-7000 Worten. Wenn man Dampfdruckkochtopf, Grippe, Brücke, Bombe, ... vermeidet, bleibt von einer normalen Unterhaltung nicht viel übrig.

Folgerung 4: Jede/r macht sich bei solchen "Kriterien" verdächtig. Niemand kann seine Unschuld beweisen, soll es aber, weil die Unschuldsvermutung bei Geheimdiensten nicht existiert. Sobald man in diese Mühlen hinein kommt, weiß man, dass man doch etwas zu verbergen gehabt hätte ...

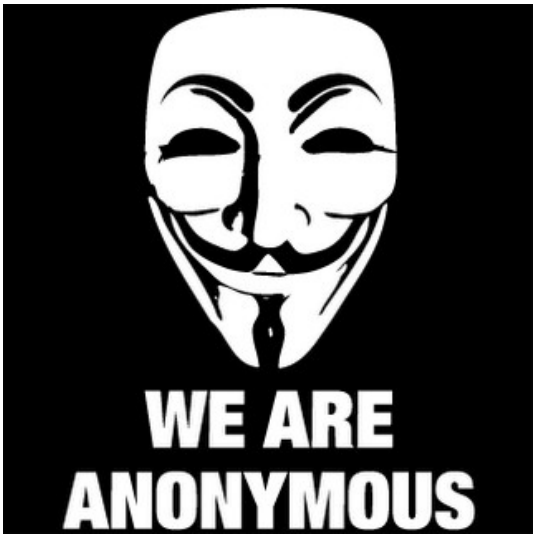
Folgerung 5: Es hat auch keinen Sinn, zu hoffen Amerika ist weit weg, auch in Europa bewegen sich Geheimdienste oft kurz hinter der Grenze des Erlaubten (Links s. oben) und auch die Polizei wird immer wieder dabei erwischt, sich Daten unerlaubt zu organisieren.

Siehe zum Beispiel

- Die EU im Cyber War?
- Britische Polizei hat Beobachtungslisten unbescholtener Bürger
- BKA setzte ausländische Spitzel ein
- BKA bestätigt europaweite Einsätze verdeckter Ermittler
- Britische Polizei testet Geodaten-Überwachung
- Nein zum staatlichen Passwort-Klau!
- Mautdaten zweckentfremden?
- Bundestrojaner als Firefox getarnt
- V-Mann Corelli belog das BKA
- Gesichtserkennung 30-mal öfter genutzt
- Antiterrordatei und Trennungsgebot
- BKA erklärt Privatsphäre für abgeschafft
- BKA-Ohr in der Leitung
- Funkzellenabfrage auch schon bei G8 Gipfel

Wie kann man sich schützen?

Wie soll man sich verhalten? - Falsche Frage, denn jede Verhaltensänderung ist auch eine Persönlichkeitsänderung. Damit zwingt uns der Staat ein Verhalten auf, das ist ein Widerspruch zum Grundgesetz, welches eine freie Entfaltung der Persönlichkeit garantiert.



Man muss wissen: nichts ist sicher,
niemand wird **nicht beobachtet**!

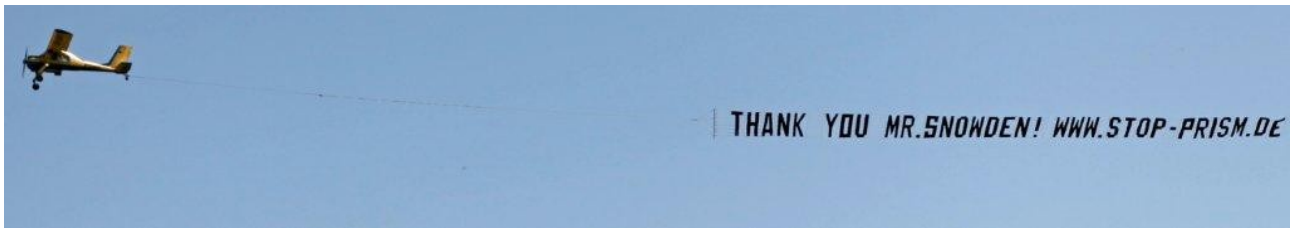
Besser als nichts ist z.B.

- keine Dienste nutzen, die in den USA beheimatet sind, also z.B. Google, Apple, Microsoft, Facebook, WhatsApp, ...

- Es gibt einfache E-Mail Verschlüsselung mit Thunderbird und Enigmail
- Mails sollte man stets mit digitaler Signatur verschicken, dann kann einem niemand etwas unterschieben, was man nicht geschrieben hat.
- Daten sollten nicht unverschlüsselt in der Cloud (kommt vielleicht von "klaut") abgelegt werden. Niemand gibt seinen Autoschlüssel einem Fremden auf der Straße.
- Anonymes Surfen geht mit Tor oder Jondonym zwar langsamer aber doch sicherer. Wer es schneller mag: Ixquick garantiert keine Daten der Nutzer zu speichern und ist in den Niederlanden zu Hause.
- Alternativen sind Programme in Open Source, also Linux, Diaspora, Libre Office, MozillaFirefox, Thunderbird, TrueCrypt, KeePassX, GnuPG, Gimp, ...
- Die EU hat Open Data verabschiedet. Alle Dateiformate von Libre Office entsprechen EU-Normen (während Microsoft Programme dies nicht tun aber massenweise genutzt werden).

Forderungen an Wirtschaft und Staat

- Der EU-Datenschutz Entwurf von Nov. 2012 war schon ganz gut. Lassen wir nicht zu, dass Industrielobbyisten und die USA ihn nach ihren Interessen verwässern. Auch Neuland-Mutti hat sich übrigens gegen den Entwurf gewandt und ihn damit weiter verzögert!
- Datensparsamkeit, Datenvermeidung - nicht alles muss gespeichert werden!
- Transparenz und Informationsfreiheit (Das Informationsfreiheitsgesetz hat noch viele Lücken!)
- Whistleblower, Journalisten und die Pressefreiheit schützen
- Vor allem sollten die europäischen Politiker endlich mal den Mut aufbringen ganz klar auszusprechen, dass wir uns eine Vollspionage durch die USA nicht länger gefallen lassen wollen - im Interesse der Menschen und ihrer Privatsphäre und auch im Interesse unserer Wirtschaft.



Update 04.07.2015: Pünktlich zum Independance Day kann man hier in den Protokollen des NSA-Untersuchungsausschusses lesen, wie wir ausspioniert werden.

Wie man sich so fühlt, wenn man ahnt oder weiß, dass ständig irgendwelche Schlapphüte in der Telefonleitung hängen oder vor der Tür stehen, beschreibt Anne Roth in ihrem Blog.

Anlässlich von Edward Snowdens Enthüllungen hat sie das noch einmal zusammengestellt.
http://annalist.noblogs.org/post/2013/09/27/innenansichten-einer-ueberwachung/