Quis custodiet custodes?

(Wer bewacht die Wächter?)

oder

Eine einfache, praxisorientierte Anleitung, wie Sie Emails und Dateien mit PGP oder S/MIME schützen können, und warum es sich lohnt, dies zu machen. Ergänzt mit Tips für eine sichere Kommunikation und Internetnutzung.

Florian Schäffer

Mit Dank für all jene, die mich bei meiner rigiden Forderung nach Verschlüsselung nicht im Stich gelassen haben und (trotzdem) PGP (widerwillig) nutzen: Angelika, Birgit, Juliane , Melanie und Sven sowie Tabea.

Inhaltsverzeichnis

1 Einleitung

Wieso das ganze?

1.1 Die 30-Sekunden-Erklärung

"Das ist zwar alles schlimm, aber solange die mir nicht an meine Geldbörse gehen, ist es mir egal."

Wenn Sie eine E-Mail schreiben und verschicken, kann jeder, der einen Teil der Internetinfrastruktur bereitstellt und über dessen Technik die Daten transportiert werden, die Nachricht lesen und verändern. Staatliche Institutionen in Deutschland, Europa und der ganzen Welt (vornehmlich in den USA) speichern jede E-Mail, die im Internet verschickt wird, dauerhaft ab und werten die Inhalte aus. Eine Zusammenstellung von Nachrichten[1] zum Thema Überwachung finden Sie im Web, wenn Sie sich weiter einlesen wollen.

Oft wird eine E-Mail mit einer Postkarte verglichen: Der Inhalt ist nicht vertraulich. Allerdings ist es bei Postkarten niemals vorgekommen, daß alle Karten durch Fremde kopiert und archiviert wurden.

Auch wenn Sie sagen "meine E-Mails interessieren doch keinen" oder "ich habe nichts zu verbergen", so ist es dennoch ratsam, Nachrichten so zu verschlüsseln, daß nur Sie und der beabsichtigte Empfänger die Nachricht lesen können. Nur so können Sie Ihre Freiheitsrechte **be**schützen. Aus reiner Bequemlichkeit auf die Möglichkeiten der Kryptographie zu verzichten, wäre ausgesprochen dumm und kurzsichtig.

Zudem bedeutet der Einsatz von Kryptographietechniken Ihrerseits keinerlei Nachteile. Sie können wie gewohnt

weiterhin per E-Mail kommunizieren – auch mit Leuten, die (noch) kein PGP oder S/MIME nutzen.

Das Bundesamt für Sicherheit in der Informationstechnik[2] spricht sich für eine Verschlüsselung von E-Mails aus: «Rechte und Freiheiten, die in anderen Kommunikationsformen längst selbstverständlich sind, müssen wir uns in den neuen Technologien erst sichern. Das Internet ist so schnell und massiv über uns hereingebrochen, daß wir mit der Wahrung unserer Rechte noch nicht so recht nachgekommen sind».

Wenn Sie jetzt neugierig sind und mehr zum Hintergrund wissen wollen, lesen Sie auch noch das nächste Kapitel: Die 60-Minuten-Erklärung oder schauen Sie sich beispielsweise das Interview[3] mit dem Whistleblower[4] Edward Snowden an oder besuchen Sie eine Webseite[5] zum Thema.

1.2 Die 60-Minuten-Erklärung

Aktueller Hintergrund

Im Sommer 2013 machen die USA Schlagzeilen durch Aufdeckung des PRISM-[6] und XKeyscore-[7] Überwachungsprogramms zur Kontrolle und Auswertung von elektronischen Medien und elektronisch gespeicherten Daten seitens der NSA. Es sind so viele Meldungen und erschreckende Aufdeckungen, daß man kaum noch folgen kann. Die USA überwachen alles.

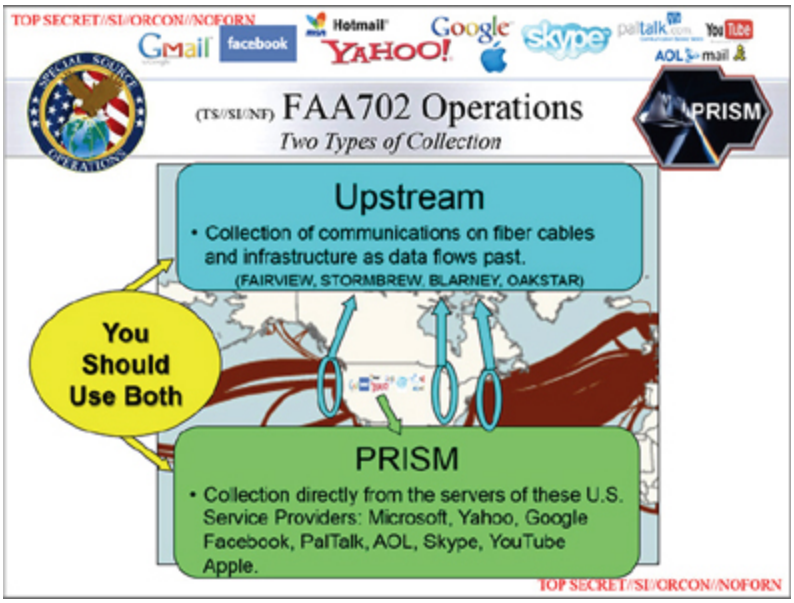
[8]

- Anrufe werden aufgezeichnet und gespeichert und nachträglich abgehört: Ex-Terrorfahnder: Keine digitale

Kommunikation ist sicher[9]

- USA: Polizeiliche Netzüberwachung ohne Richterbeschluss[10]
- US-Regierung zapft Kundendaten von Internet-Firmen an[11]
- Whisteblower Snowden lieferte tausende Dokumente über PRISM[12]
- Facebook und Microsoft informieren ein wenig über NSA-Anfragen[13] (bei der Vielzahl an Abfragen ist es rein rechnerisch gar nicht möglich, daß jedesmal ein Richter sein OK gab)
- NSA-Überwachungsskandal: Von PRISM, Tempora, XKeyScore und dem Supergrundrechtr – was bisher geschah[14]
- Zwischenruf: Warum die NSA-Affäre alle angeht[15]. Eine leicht verständliche Zusammenfassung die etwas weniger polemisch ist, als mein Text.
- NSA-Überwachungsskandal: Von NSA, GCHQ, BND, PRISM, Tempora, XKeyScore und dem Supergrundrecht – was bisher geschah[16]
- World Wide War. Wie mit Hinweis auf die Terrorabwehr das Post- und Fernmeldegeheimnis verletzt wird und wie private Räume immer mehr öffentlich werden. ZDFinfo Video[17]

Jede E-Mail, jede Webseite, jeder Webseitenabruf, jede Suchanfrage, jedes Telefonat, jede SMS ist betroffen. Deutlich macht dies eine Grafik der NSA aus einem Artikel der Washington Post:



18

Mit "Upstream" wird die gesamte Kommunikation auf den transatlantischen Datenleitungen abgegriffen. "PRISM" sammelt Daten in den USA direkt von den Servern von Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube und Apple.

Und immer noch gibt es Leute, die behaupten, sie hätten ja nichts zu verheimlichen, es sei doch gut, wenn dadurch die Bösen gefunden würden. Nur: Wer entscheidet, wer zur Achse des Bösen[19] gehört? So viele Kriege[20], Demonstrationen[21], Aufstände[22] usw. wurden von den Machthabern als Angriff auf sonst was bezeichnet, wurden aber zumindest von der "freien Welt" als positiv gewertet und führten im Nachhinein betrachtet in die Freiheit, zu Demokratie und Menschenrechten etc. - oder auch zu noch mehr staatlicher Unterdrückung. In der Türkei werden 2013 mehr oder weniger harmlose Demonstranten von der eigenen Regierung als Terroristen[23] betitelt. Das Wort *Terrorist* sitzt seit 9/11 ziemlich locker bei Regierungen und Sicherheitsorganen. Wann ist das, was bisher eine harmlose Kommunikation war, ein terroristischer Akt? Die Einwanderungsbehörde der USA kann jeden Einreisenden bei kleinstem Verdacht an der Grenze oder schon beim

Abflug[24] aus einem anderen Land ohne Begründung abweisen[25] - unter dem Deckmantel der Terrorismusbekämpfung. Die USA haben Angst! Ein ganzes Land scheint unter dem Dogma zu leben, daß überall um sie herum das Böse nur darauf wartet, sich über die Bürger herzumachen.

Früher exportierten die USA neue Trends, eine neue Weltanschauung und den American Way of Live. Heute exportieren sie Angst. Und alle Länder lassen sich anstecken. Aus Angst vor einer möglichen Gefahr, die keiner genau beschreiben kann, die keiner kennt und über die keiner redet, weil er zum Stillschweigen verdonnert ist, lassen wir uns in unseren Freiheiten beschneiden, nehmen immer mehr Überwachung und Kontrolle in Kauf und lächeln über die, die Orwell[26] zitieren. Ist doch (noch!) alles nicht so schlimm, das hat doch seine Berechtigung, das ist zum Wohle der Allgemeinheit.

Und was haben wir davon? Weniger Angst? Nein.

Wir leben in einer Diktatur, wenn wir uns von anderen diktieren lassen, daß wir Angst haben sollen, daß wir ständig bedroht werden. Hätten Sie Angst, wenn der Terror nicht mindestens einmal täglich irgendwo breitgetreten werden würde? Ich habe keine Angst vor einer nicht greifbaren, abstrakten Gefahr. Ich habe angst davor, daß wieder einmal meine Rechte beschnitten werden. Zumal unsere Demokratie nicht ohne Grund auf dem Prinzip der Gewaltenteilung[27] basiert. Wenn aber ein Geheimdienst zusammen mit dem US-Geheimgericht FISC (Foreign intelligence Surveillance Court) (Jurisdiktion) sich willkürliche Gesetzte (Legislative) ausdenkt und diese mit eigenen Geheimdienstmitarbeitern auch noch durchsetzt (Exekutive), dann wird das (bei uns im Grundgesetz Artikel 20[28] verankerte) Modell ad absurdum geführt und die genannten Organe handeln widerrechtlich.

"Das alles führt zur Einschüchterung der Nutzer. «Chilling Effects» nennt man es, wenn allein das Wissen, dass Überwachung, zumal flächendeckende, stattfinden könnte, zu vorauseilendem Gehorsam führt. Wenn sich Nutzer fragen, ob die Nachricht, die sie schreiben, das Video, das sie anschauen, die Lektüre des Textes, den sie lesen, nicht irgendwann gegen sie verwendet wird. Und dann die Nachricht nicht schreiben, den Text nicht lesen, das Video nicht gucken. Wer so aus Angst vor Folgen handelt, ist fremd im eigenen Haus. Er ist auch kein Bürger mehr. Er ist ein Untertan."[29]

"Die weitläufige Überwachung von Telefonverbindungen und des Internet durch amerikanische Geheimdienste hat nach Angaben der US-Behörden in den vergangenen Jahren etwa 50 Terror-Verschwörungen in 20 Ländern vereitelt."[30] In einem einzelnen Jahr (bspw. 2008) gab es in den USA 702.907 Verbrechen und Vorfälle[31] und 10.869 Tötungsdelikte[32] mit Schußwaffen[33]. Trotzdem redet kein amtierender Politiker und kein Überwachungsfanatiker davon, die NRA[34] zu verbieten oder besser zu kontrollieren/zu überwachen oder gar die Wahlkampfversprechen zum verschärften Waffenbesitzrecht umzusetzen. In Deutschland waren es immerhin auch 171 Tötungen[35]. Mehr Menschen als je durch einen Terroranschlag hierzulande starben, und dennoch werden Unsummen an Steuergeldern zur totalen Überwachung der Bürger mit der Begründung zur Terrorabwehr ausgegeben bei gleichzeitig ziemlich laxen Waffenbesitzrecht.

Und wohlgemerkt: Es geht um "Verschwörungen" nicht Attentate! Nachprüfen kann das keiner. Wieviele Menschen wären dabei vielleicht gestorben? Und es geht auch nicht um die Überwachung von Verbrechern. Solche sind nämlich verurteilt und dürfen im gesetzlichen Rahmen durchaus überwacht werden. Die ganze Überwachung richtet sich gegen *Verdächtige.* Wer aber verdächtig ist und wieso,

unterliegt dabei ausschließlich einer subjektiven Betrachtung. Jeder kann sehr schnell zum Verdächtigen werden – ganz unabhängig davon, ob er objektiv betrachtet wirklich ein Verbrechen begehen will.

Aber nicht nur die USA spionieren. Auch die deutschen[36] (und viele andere[37] Staaten[38] auch) und sie wollen immer mehr Daten durchforsten. Vorreiter im negativen Sinn sind neben der NSA hier u. a. der französische Auslandsnachrichtendienst Direction Générale de la Sécurité Extérieure (DGSE) und das britische Government Communications Headquarters (GCHQ).

"2011 hatte der Bundesnachrichtendienst fast 2,9 Millionen E-Mails und SMS wegen des Verdachts auf Terrorismus, Waffenoder Menschenhandel überprüft."[39]

Und (angeblich) haben die deutschen Politiker nicht einmal davon gewußt[40], daß sie selbst von den Briten ausgeschnüffelt werden. Es werden sogar Lügen wie "es werden normale Bürger nicht ausspioniert"[41] vom ehemaligen Bundesinnenminister Hans-Peter Friedrich (CSU) verbreitet. Da fragt man sich doch, wozu die eigene Schnüffelei gut ist, wenn man nicht einmal den Feind im eigenen Bett erkennt[42]. Aber vermutlich hätte man dazu einfach noch mehr Nachrichten "überprüfen" müssen. Ist doch eigentlich eine gute Argumentation: "Wir brauchen die totale Überwachung, damit wir die totale Überwachung anderer überwachen können".

Die Vogel-Strauß-Nutzer werden auch dies nicht als störend empfinden. Aber sie sollten sich überlegen, wie es weitergeht: Britische Internet-Provider müssen Porno-Filter einsetzen[43]. Das ist Zensur[44]! Wer Pornos zensieren[45] kann, hat die Technik zur Hand, alle anderen Inhalte auch zu zensieren. Die Zensur erfolgt nämlich auf der Basis einer Liste von Webadressen und Wortlisten[46] und nicht nach der

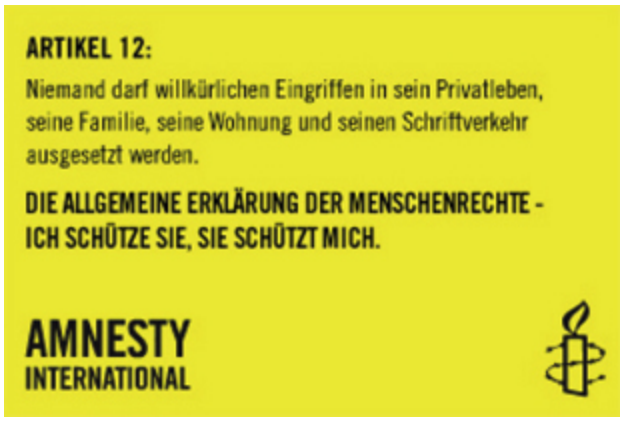
Analyse tatsächlicher Inhalte. Wer entscheidet, was zensiert werden darf oder wie weit wir entmündigt werden dürfen?

Für Frieden, Freiheit, Öl und Waffengeschäfte opfern wir tausende Zivilisten und Soldaten bereitwillig. Vielleicht sollten wir lieber auch ein paar Opfer durch Verschwörungen akzeptieren, bevor wir hinnehmen, daß wir (wieder) in einem Überwachungsstaat leben. Gänzlich[47] verhindert[48] hat die ganze Schnüffelei nämlich gar nichts[49]. Es gab schon immer Tote, weil andere ihre Ideologie (von Glauben[50], Frieden[51], Gerechtigkeit[52] usw.) nicht mit Worten durchsetzen konnten, sondern lieber zur Waffe griffen. Wieso werden für den kläglichen Versuch Frieden zu erzwingen viele Freiheiten, für die unsere Vorfahren und Mitmenschen gekämpft haben, die in unserer Verfassung oder dem Grundgesetz garantiert sind, auf dem Altar der Terrorismusbekämpfung geopfert[53]?

Es ist schon peinlich: Ein Staat, der sonst vermeintliche Feinde ohne Gerichtsverfahren oder Zubilligung von Menschenrechten[54] einfach entführt[55] und verschleppt, bettelt bei den Mächten, die er vorher ausgespäht[56] und so gegen sich aufgebracht hat, nun darum, daß ihm ihr derzeitiger Staatsfeind Nr. 1[57] ausgeliefert wird.

"[US-Außenminister John Kerry] drängte Russland demnach dazu, sich an die juristischen Standards zu halten, "denn das ist in jedermanns Interesse."[58]

Datenschutz und Privatsphäre sind dann wohl keine Standards in jedermanns Interesse, sondern Werkzeuge des Terrorismus. Und trotz der allumfassenden Überwachung wissen die Behörden nicht einmal, wo sich "der böse Verräter" gerade aufhält.



59

«Bundesinnenminister Friedrich hat der Sicherheit Vorrang vor allen anderen Grundrechten eingeräumt, auch der Freiheit. "Sicherheit ist ein Supergrundrecht", das gegenüber anderen Rechten herauszuheben sei, erklärte der CSU-Politiker. Obwohl er noch versucht hat, diese Aussage zu relativieren, scheint er die Grundrechte damit zu Privilegien zweiter Klasse entwerten zu wollen. Dabei stehen sie gerade als Abwehrrechte gegen Eingriffe des Staates in der Verfassung. Sein Parteikollege Hans-Peter Uhl, Innenexperte der Unionsfraktion, bezeichnete das Recht auf informationelle Selbstbestimmung gar als eine "Idylle aus vergangenen Zeiten".»60

«Das Nachrichtenmagazin Der Spiegel berichtete61 vom Angriff der NSA und der GCHQ auf Smartphones (Blackberry, iPhone, Android). Eigenen Angaben zufolge können die Geheimdienste auf die Betriebssysteme zugreifen und dabei nahezu alle sensiblen Informationen eines Smartphones auslesen. In Bezugnahme auf den Roman 1984 von George Orwell fragt eine interne NSA-Präsentation, "wer sich im Jahr 1984 hätte vorstellen können, daß Steve Jobs der wahre Große Bruder sein würde und die Zombies zahlende Kunden sind." Zu den auslesbaren Informationen gehören die Kontaktlisten, die Kurzmitteilungen, Daten verschiedener Anwendungsprogramme, Notizen und der aktuelle Aufenthaltsort des Smartphones. Die vom Spiegel eingesehenen Materialien legen den Schluß nahe, daß es

sich nicht um Massenausspähungen handelt, sondern um zielgerichtete, teils auf den Einzelfall maßgeschneiderte Operationen, die ohne Wissen der betroffenen Unternehmen laufen.»[62] Das ganze wird dann auch noch mit drei Bildern untermalt, die jeden Apple-Kunden verhöhnen und zeigen, welche perfiden Gedanken die Geheimdienste haben (und dabei tatkräftig durch die Apple-Jünger unterstützt werden):

Erstes Bild[63]:

"Wer hätte sich 1984 vorstellen können..."

(Werbespot[64] "1984" von Apple zur Einführung des Macintosh)

Zweites Bild[65]:

"...daß dies Big Brother sein würde..."

(Steve Jobs von Apple mit einem iPhone in der Hand)

Drittes Bild[66]:

"...und die Zombies zahlende Kunden sind?"

(iPhone Kunden, die auch beim neuen Update wieder dem Hype[67] verfallen.)

Und während die europäische Politik die Bürger nicht aufklärt[68], sondern sich mit Plattitüden abspeisen läßt, keine Gegenmaßnahmen ergreift und die Sache eher unter den Teppich kehren will, obwohl ein EU-Bericht vor der massiven Gefahr für die Demokratie[69] warnt, wird unsere Freiheit wohl eher am Amazonas verteidigt[70], als durch unsere Politiker oder Bürger.

Die Fragen, die sich angesichts dieser eskalierenden Totalüberwachung stellen, sind folgende:

Kann ich etwas gegen die Datenspeicherung und Auswertung meiner E-Mails, Telefonate, Kurznachrichten, Internetaktivitäten usw. unternehmen?

Nein. Egal, welche Partei man wählt oder wie viele Demonstrationen abgehalten werden: Selbst wenn sich die Bundesdeutsche Regierung von einem Paradigmenwechsel überzeugen lassen würde, so interessiert das andere Regierungen nicht. Staaten, in denen die Überwachung bereits etabliert ist (z. B. Großbritannien, USA, China),

werden nicht aufhören, immer mehr Daten zu sammeln und die Techniken zu verfeinern. Sie werden sich dabei auch über die Respektierung von besonders geschützten Berufsgruppen wie Journalisten[71] hinweg setzen und diese sogar als "potenzielles Sicherheitsrisiko[72]" einstufen. Auch an internationale Abkommen halten sich diese Länder nicht – immerhin ratifizieren sie auch andere Gesetze[73] nicht und fordern schon jetzt immer mehr Daten[74] ein. Und selbst die EU kriecht vor den Überwachern auf dem Boden. Delegierte werden daran gehindert[75], die Rechte der EU-Bürger zu verteidigen oder sich zu informieren. Da man als Anwender so gut wie keine Kontrolle darüber hat, welche Server in welchen Ländern die Daten im Internet transportieren, kann man es nicht verhindern, daß sich in der Reihe ein Knoten auch ein System im Ausland befindet (selbst wenn z. B. die E-Mail von einem Deutschen Anwender in Deutschland an einen Empfänger in Deutschland geschickt wird) oder ein ausländisches Unternehmen diesen Knoten kontrolliert oder ein Datensammler die Daten an diesem Knoten (heimlich) abgreifen kann oder die Daten sogar aktiv im Rahmen von Reglementierungen an einen ausländischen Geheimdienst etc. weitergeleitet werden.

Gefahr lauert aber nicht nur da, wo Staaten Daten aus Kommunikationsnetzwerken abgreifen können. Auch das Betriebssystem des PCs sorgt für mangelnde Sicherheit oder öffnet den Behörden heimtückische Hintertüren. Ein Stichwort ist der sogenannte Staatstrojaner[76]: Eine staatliche Software, die heimlich auf dem Computer installiert wird und dann den Vollzugriff auf alle Dateien und Aktivitäten ermöglicht. Eine andere Hintertür[77] kommt mit Windows 8 und nennt sich Trusted Computing: Zusammen mit einer speziellen Hardware in Form eines Chips – dem Trusted Platform Module (TPM), der bei zukünftigen PCs serienmäßig installiert sein wird, hat der Betriebssystemhersteller (in dem Fall Microsoft)

uneingeschränkten Zugriff auf den Computer. Und wenn Microsoft Zugriff hat, dann hat es auch die NSA – das befürchtet selbst das Bundesamt für Sicherheit in der Informationstechnik (BSI). Wer dem entgehen will, sollte auf Windows 8 und/oder auf einen Computer mit integriertem TPM verzichten.

Manchmal lauert die unerwünschte Datensammlung aber auch an Stellen, an denen man es eher weniger erwartet und bei Institutionen, denen man naturgemäß eigentlich vertraut, zumal hier das Briefgeheimnis greifen sollte. Aber die Deutsche Post[78] (und vermutlich auch viele andere nationale und internationale Briefdienstleister, wie es zum Beispiel vom U.S. Postal Service[79] bekannt ist) scannen bei jeder Sendung die Adresse und digitalisieren die Daten. Das dient natürlich in erster Linie der schnellen Sortierung. Damit der aufwendige Scanvorgang (und vor allem die ggf. sogar manuelle Schrifterkennung) nur einmal pro Sendung notwendig ist, wird danach ein sogenannter Zielcode [80]mit fluoreszierender oranger (o. ä.) Farbe aufgedruckt. Anschließend kann bei allen weiteren Sortierschritten anhand des Strichcodes die Sendung bearbeitet werden. Es ist also in keiner Weise notwendig, die ermittelten Adreßdaten weiterhin abzuspeichern. Genau das wird aber gemacht: Alle Daten werden gespeichert und sogar an andere Unternehmen und Geheimdienste weitergegeben – ganz ohne richterlichen Beschluß. So kennt der Geheimdienst zwar nicht den Inhalt des Briefes aber weitere Metadaten, aus denen sich Profile erstellen lassen.

Manchmal sind wir sogar selber bereit unsere Privatsphäre aufzugeben. Nur um ein paar Euro zu sparen, installieren wir dann Überwachungstechnik und liefern uns der Willkür von Unternehmen aus, die nicht müde werden, uns vermeidliche Vorteile zu verkaufen, während sie die gewaltigen Nachteile herunterspielen: Versicherungstarif[81] mit GPS-Überwachung, Dashcams[82], Pay-back[83], Google Latitude[84] (Google+,

Glympse usw.), Google Screenwise[85], um nur einige zu nennen.

Warum ist es denn nun schlimm, wenn jemand meine privaten E-Mails liest und meine Fotos ansehen kann?

Es ist nur schwer, hierfür wirklich greifbare Argumente zu finden. Natürlich ist es im Grunde belanglos, wenn die NSA erfährt, daß Sie alle Ihre Freunde zum Geburtstag einladen oder wenn jemand beim Internetprovider (z. B. der Telekom, AOL usw.) Ihre Urlaubsfotos anschaut. Das am häufigsten ins Feld geführte Argument lautet dann "Ich habe doch nichts zu verbergen". Denken Sie immer daran, denn große E-Mail-Anbieter sehen das genau so: Wer ein E-Mail an einen Gmail-Nutzer schickt, verzichtet auf Privatsphäre[86]. Leider bietet die Technik und die Menge an Daten auch viel Potential für Mißbrauch, und Politiker, sowie Geheimdienstmitarbeiter beweisen leider immer wieder, daß sie das in sie gesetzte Vertrauen mißbrauchen und zu rein privaten Zwecken[87] ihre Nase in Dinge stecken, die sie gar nichts angehen und wofür sie keine Berechtigung haben – aus reiner Eifersucht, Neugier, Unwissenheut und Dummheit oder Ignoranz.

Vor 25 Jahren gingen die Leute noch auf die Straße und erkämpften im sogenannten Volkszählungsurteil[88] die Anerkennung des informationellen Selbstbestimmungsrechts als vom Grundgesetz geschütztes Gut. Damals ging es darum, daß der Bürger wissen soll und darf, wer was wann und bei welcher Gelegenheit über ihn weiß. Heute leben wir in einem Polizeistaat[89] und überblicken die Konzentration an dauerhaft irgendwo von einem Staat gespeicherten (jeder einzelne für sich genommenen banale) Informationshappen, die wir selbst

nicht kontrollieren können und von denen wir nicht wissen, wer ihm im nächsten Jahr kontrolliert, in keiner Weise mehr.

"Die Gesellschaft muß akzeptieren, daß der Preis der Freiheit eine gewisse Unsicherheit ist. [...] Und selbst wenn es gelungen wäre, die Anschläge [beim Marathon in Boston] zu verhindern: [...] Wäre es das Wert, unsere Gesellschaft in einen Überwachungsstaat zu verwandeln? [...] Wir haben in den USA nach den Terroranschlägen überreagiert und damit sehr viel Schaden angerichtet. Der Schaden dadurch war sogar noch größer als durch die Anschläge selbst. Wir haben unsere demokratischen Institutionen beschädigt."[90]

Wäre es Ihnen nicht auch unangenehm, wenn Ihre normale Post geöffnet würde und ein Polizist jeden Brief, jede Rechnung jeden Kontoauszug, Ihre Wahlunterlagen durchliest? Oder wenn die Kassiererin im Supermarkt alle Fotos durchsieht, die in der Fotoabteilung zur Abholung liegen? Aus dem Lesen Ihrer Rechnungen oder dem Liebesbrief Ihres Freundes, Ihrer Freundin entsteht noch kein Schaden aber welche Möglichkeiten ergeben sich daraus? Nicht ohne Grund gibt es das Briefgeheimnis und es ist ein Grundrecht. Es geht dabei nicht um den Schutz von Geheimnissen, sondern um den allgemeinen Schutz der Privatsphäre.

"Man gebe mir sechs Zeilen, geschrieben von dem redlichsten Menschen, und ich werde darin etwas finden, um ihn aufhängen zu lassen."[91]

"Alles in allem scheinen die westlichen Geheimdienste zu einem supranationalen und antidemokratischen Monster zu mutieren, für das rechtsstaatliche Schranken immer weniger gelten. Vor diesem Hintergrund ist es der Skandal im Skandal, dass sich in Deutschland, dem Land, in dem mit der Gestapo und der Stasi bereits zwei übermächtige Geheimdienste ihr Unwesen getrieben haben, nicht viel mehr Widerstand rührt."[92]

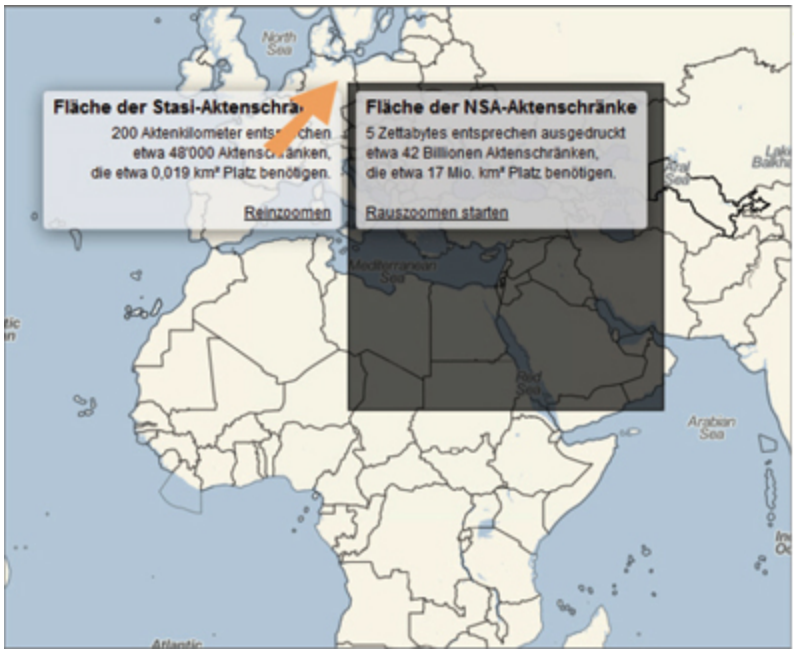
Man kann sich auch andersherum fragen:

Wieso sammeln die Behörden so viele Daten?

Wenn doch die E-Mail an Tante Erna keine Geheimnisse enthält, warum wird sie dann von der NSA und anderen Behörden abgefangen, analysiert und gespeichert?

Begründet wird die Sammelwut stets damit, daß man nur so Verbrechen und Terrorakte verhindern kann. Wie bereits ausgeführt, kann man aber gar nicht alle Verbrechen verhindern. Eine weitere Stellungsnahme[93] zur Frage, wie oft Telefondaten eindeutig bei der Unterbrechung eines Terrorplans geholfen hätten, zeigt, wie traurig das Ergebnis ist: In 54 Fällen seien nur 13 durch die USA nachverfolgt worden und davon habe man nur 12 Fälle teilweise, aufdecken können. Wieder: kein Wort von Vereitelung, man hat lediglich davon gewußt. Dazu wurden aber Millionen von Telefondaten gesammelt und gespeichert. Ein ähnliches Problem gibt es bei der Videoüberwachung: Es werden keine Verbrechen durch vermehrte Überwachung verhindert und auch die Aufklärungsquote[94] ist nur unwesentlich besser. Primär geht es dabei darum, den Menschen ein subjektives Gefühl von Sicherheit zu vermitteln.

opendatacity.de vergleicht die Sammelwut von Stasi und NSA in einer Grafik, die anschaulich zeigt, wie unvorstellbar gigantisch die Datenmenge ist, die allein die NSA speichern kann. Wenn man alle Daten ausdrucken würde, füllte die Stasi "nur" Aktenschränke mit einer Stellfläche, die in der abgebildeten Landkarte nicht einmal einen einzelnen Punkt beanspruchen würde (Pfeil). Die Aktenschränke der NSA bräuchten eine Fläche (dunkelgrau) größer als Australien. Was wollen sie mit diesen Daten anfangen?



95

„Aber in meiner E-Mail an Tante Erna steht doch gar nichts über ein Verbrechen?“

Sicher nicht. Auch ist auf den Fotos vom Urlaub nichts Verdächtiges abgebildet. Aber man kann ja nie wissen, wann eine Bemerkung, die heute vielleicht noch unproblematisch ist, oder ein Foto, daß einen harmlosen Ausflug zu einem Kulturdenkmal zeigt, nicht doch mal auf illegale Aktivitäten hinweist. Die Gesetze und Zielgruppen, nach denen gefahndet wird, können sich jederzeit ändern. Vielleicht ist es in ein paar Jahren verboten, sich über einen Politiker lustig zu machen oder in das Land mit dem Kulturdenkmal einzureisen. Jeder, der vor ein paar Jahren so etwas gemacht hat (als es noch völlig in Ordnung war), ist aus der neuen Sicht dann suspekt. Da Sie nicht wissen, wer Ihre Daten sammelt, können Sie auch nicht sicher sein, wie sich die Politik in diesem Land verändert.

Das Problematische ist die Heimlichkeit mit der das passiert, der Umfang und die Tatsache, daß die Daten ausgewertet und für alle Ewigkeit gespeichert werden, sowie die immer stärker um sich greifende technische Verbesserung[96]. Vor

allem auch die (automatisierte) Analyse der Daten kann aus völlig harmlosen Einzelfällen ein verzerrtes Gesamtbild entstehen lassen, in dem Sie dann auf einmal als suspekte Person dastehen und sich ggf. gegenüber Behörden rechtfertigen oder Repressalien über sich ergehen lassen müssen. Hierfür kann man sich viele Beispiele ausdenken und es gibt bereits immer wieder Hinweise darauf, daß es genau so kommen kann: Die Einreise in die USA wurde verweigert[97], weil die Daten im Onlinebuchshop Amazon verdächtige Interessen vermuten lassen. Vielleicht haben Sie sich auch schon mehrmals über Freiheitsrechte, Amnesty International, Bürgerkriege und ähnliches bei Twitter oder Facebook ausgetauscht? Egal wie harmlos einzelne Daten sind: In der Summe kann sich ein völlig neues (falsches) Bild von Ihnen ergeben: Sie schreiben Tante Erna von dem Schnupperkurs im Flugsimulator, twittern den Kauf Ihres neues Kopftuches für den Sommerurlaub, lassen sich per E-Mail Flugangebote für selbigen in den Nahen Osten schicken, suchen nach Informationen zum neuen 787 Dreamliner von Boeing (dem zweitgrößten Rüstungskonzern der Welt) für Ihren Flug, bestellen das vegetarische Bordessen, lesen Online etwas über Terroranschläge im Irak, sprechen mit Ihrem Freund am Handy über Ihre Sorgen, in Ägypten entführt zu werden und lassen sich von der Google-Übersetzungsapp ein paar Fotos mit arabischen Schriftzeichen am Urlaubsort übersetzen. Diese Kommunikation wurde über Monate hinweg komplett protokolliert, gespeichert und analysiert. Na, welches Bild kann man jetzt von Ihnen haben? Wäre es nicht vielleicht lohnenswert, Ihre Urlaubsfotos, die sie online im Fotolabor bestellen oder per E-Mail an die Freunde schicken, zu sichten, um dort nach Ausbildungscamps für Terroristen zu schauen? Und auch, wenn man nichts Verdächtiges findet – denn Sie sind ja kein Terrorist und haben nichts zu verbergen: es kann sich lohnen, Ihren Bekanntenkreis näher unter die Lupe zu nehmen oder Sie bei der nächsten

Einreise in die USA oder bei der Polizeikontrolle in London ein wenig stärker zu filzen. Das Bundeskriminalamt (BKA) erfaßte und speicherte allein im Jahr 2014 zum Beispiel 1,5 Millionen personengebundener Hinweise (PHW) zu Bürgern ohne Vorstrafen. An sich belanglose Hinweise[98] auf Stichworte wie "Ansteckungsgefahr“, "geisteskrank“, "gewalttätig“, "Land/Stadtstreicher“, "Prostitution“ und "Rocker“ können schon dazu führen, daß auch Sie lebenslang in dieser Datenbank landen.

Die aktuelle Entwicklung[99][100][101] holt sie schneller ein, als Ihnen recht ist: In New York (USA) wurde eine Hausfrau von (Polizei-) Beamten einer Joint Terrorism Task Force aufgesucht, die sich bei ihr über mögliche terroristische Aktivitäten informieren wollte und ihre Wohnung durchsuchte. Die Familie verhielt sich suspekt, weil verschiedene Suchanfragen im Internet nach Schnellkochtöpfen, dem Boston-Marathon-Attentat, Rucksackreisen und einem ominösen "Quinoa"[102] bei den Agenten ins Raster für kriminelle Handlungen paßten. Angeblich sollen etwa 100 derartige Hausbesuche pro Woche stattfinden – bei 99 % seien sie ergebnislos.

Auch wenn es sehr provokant sein mag: Ein in den Ausweis[103] gestempeltes "J" ist noch nicht weiter dramatisch. Vielleicht kann man auch noch über einen gelben Stern am Revers hinwegsehen – man hat ja nichts zu befürchten, man ist ja ein guter Mensch, ist produktiv, zahlt Steuern und ist gesetzestreu. Aber wenn all die "harmlosen" Schritte nur dem Ziel dienen, die Menschen zu erkennen, die vernichtet werden sollen, dann ist es zu spät, wenn man dies erkennt.

Die Geschichte zeigt: Regierungen ändern andauernd ihre Meinung, politische Partner werden schnell zu Feinden. Ideologien kehren sich ins Böse. In der Historie hat noch kein Land dauerhaft eine politische Linie beibehalten. Wollen Sie wirklich einem Land Ihre Daten dauerhaft anvertrauen, in dem die Rassendiskriminierung[104] noch keine 60 Jahre her ist? Oder in dem Menschen noch immer an die Wand gestellt und erschossen[105] werden? Der Schritt zum autoritären Polizeistaat ist nicht sehr groß und wer möchte schon in einer Welt leben, wie sie Sciencefiction[106] Autoren[107] längst heraufbeschworen[108] haben? "Vielleicht nicht heute, vielleicht nicht morgen, aber bald und dann für den Rest deines Lebens."[109] Die jährlich vergebenen Big Brother Awards[110] zeigen, daß die Überwachung inzwischen fast alle Bereiche des Alltags erreicht hat und selbst Kinder ausgehorcht werden. Oft handeln die Verantwortlichen dabei in vermeintlich guten Interesse und überschreiten eher unbewußt die Grenzen des Akzeptablen oder des Rechts. Das ist dann aber nicht weniger schlimm, denn es zeigt, daß das Unrechtbewußtsein immer mehr aufgeweicht wird und jeder glaubt, Daten sammeln zu dürfen und zu müssen.

Es sind aber auch nicht immer nur Staaten und Geheimdienste, die Daten sammeln und mißbrauchen. Die Privatwirtschaft sammelt mit Eifer Daten von Bürgern, um Verhaltensprofile, Risikoabschätzungen und Werbung zu verkaufen. Das ist nicht immer legal, wird aber oft sehr milde bestraft, selbst wenn Justizbeamte[111], denen man ja

eigentlich auch vertrauen können sollte, intimste Details verkaufen. Unsere Daten sind nirgends sicher – es gibt immer jemand, der begehrlich darauf ist.

Kennen Sie Thelma Arnold? Vermutlich nicht. Aber eigentlich können Sie über diese US-Amerikanerin fast alles im Web erfahren. Das liegt nicht daran, daß diese ältere Frau alles über sich selbst veröffentlicht hat. Es liegt daran, daß Internetdienstleister so viele Daten über jeden Nutzer – also auch über Sie – sammeln, daß selbst anonymisierte Daten sich wieder zu einem Profil zusammensetzen lassen. So geschehen im August 2009: AOL veröffentlichte die über 20 Millionen anonymisierten Suchanfragen von 657.000 seiner Kunden als Demonstration, wie sicher diese Daten doch angeblich sind. Das weckte die Neugier eines Journalisten der New York Times[112]. Er durchforschte die Protokolle aufmerksam und setzte das Puzzle zusammen: "Die Kundin des Providers AOL mit der Benutzernummer 4417749 interessierte sich beispielsweise für „60-jährige Single-Männer“ und litt unter „tauben Fingern“ und einem „Hund, der überall hinpinkelt“. Sie suchte einen „Gärtner in Lilburn, Georgia“ und „zum Verkauf stehende Häuser im Stadtteil Shadow Lake“. Später gab sie den Namen ihres Sohnes in die AOL-Suchmaschine ein: Er heißt Arnold mit Nachnamen. In Shadow Lake leben elf Arnolds. Nur wenige Anrufe führten den Reporter zur 62-jährigen Thelma Arnold."[113] Können Sie sich ausmalen, was jemand, der seit Jahren Zugriff auf alle Suchanfragen der großen Anbieter hat, mit den Daten anfangen kann? Und wollen Sie, daß diese Daten zu irgendeinem Zeitpunkt in die Hände derer kommen, die über Ihr Wohlergehen entscheiden? Was heute, hier völlig harmlos sein mag, kann morgen, woanders eine Straftat sein oder Sie verdächtig machen. Homosexuelle haben beispielsweise seit Juni 2013 in Rußland[114] nicht mehr das Recht, sich im Internet positiv zur Homosexualität zu äußern – dazu gehören auch E-Mails. In einer Scheindemokratie wie

Rußland kann das auch genutzt werden, um unliebsame Bürger zu verfolgen, die sich früher einmal mit dem Thema aus beliebigen Gründen beschäftigt haben. Wer garantiert Ihnen, daß es nicht irgendwann auch Sie trifft? Derartige mittelalterlichen politischen Entscheidungen und Gesetzesänderungen kann es in jedem Land geben.

Aber es ist doch gut, wenn Terrorakte verhindert werden können

Keine Frage, das ist es. Aber genau dieser Erfolg stellt sich ja nicht (oder nur minimal) ein: "Obama-Berater: NSA-Vorratsdatenprogramm hat keine Anschläge verhindert[115]". "Bisher sei noch kein Anschlag dadurch verhindert worden, sagte Snowden[116] […].

Frankreich habe seit vergangenem Jahr das umfassendste Abhörgesetz in Europa […]. «Dennoch hat dies die Anschläge *[in Paris]* nun nicht verhindern können.» Regierungen investierten zu viel Geld und Energie in die Erfassung und Analyse von Daten […]." Und es ist eben unverhältnismäßig, wenn man die Freiheitsrechte aller Menschen weltweit beschneidet, nur um ein paar Straftäter zu ermitteln. Man könnte auch einfach alle Menschen präventiv in Isolationshaft stecken – nur um Einzelne davon abzuhalten, ein Verbrechen zu begehen: "Verhaftet die üblichen Verdächtigen!"[117] Die Frage für eine rechtsstaatliche Demokratie bleibt: wieviel Freiheit ist man gewillt aufzugeben, um ein wenig Sicherheit zu gewinnen? Oder, um es mit einem der Väter der amerikanischen Unabhängigkeitserklärung, Benjamin Franklin zu sagen: "Wer wesentliche Freiheit aufgeben kann um eine geringfügige bloß jeweilige Sicherheit zu bewirken, verdient weder Freiheit, noch Sicherheit."[118]