

Inhaltsverzeichnis

1	Einleitung	1
2	Beispiel Google	2
3	User-Tracking	8
4	History Sniffing	10
5	Geotagging	11
6	Kommunikationsanalyse	13
7	Überwachungen im Internet	14
8	Rechtsstaatliche Grundlagen	18
9	Ich habe doch nichts zu verbergen	19

1 Einleitung

Im realen Leben ist Anonymität die tagtäglich erlebte Erfahrung. Wir gehen eine Straße entlang, kaufen eine Zeitung, ohne uns ausweisen zu müssen, beim Lesen der Zeitung schaut uns keiner zu.. Das Aufgeben von Anonymität (z.B. mit Rabattkarten) ist eine aktive Entscheidung.

Im Internet ist es genau umgekehrt. Von jedem Nutzer werden Profile erstellt. Websitebetreiber sammeln Informationen (Surfverhalten, E-Mail-Adressen), um beispielsweise mit dem Verkauf der gesammelten Daten ihr Angebot zu finanzieren. Betreiber von Werbe-Servern nutzen die Möglichkeiten, das Surfverhalten websiteübergreifend zu erfassen.

Verglichen mit dem Beispiel *Zeitungslesen* läuft es auf dem Datenhighway so, dass uns Zeitungen in großer Zahl kostenlos aufgedrängt werden. Beim Lesen schaut uns ständig jemand über die Schulter, um unser Interessen- und Persönlichkeitsprofil für die Einblendung passender Werbung zu analysieren oder um es zu verkaufen (z.B. an zukünftige Arbeitgeber). Außerdem werden unsere Kontakte zu Freunden ausgewertet, unsere Kommunikation wird gescannt. . .

Neben den Big Data Firmen werden auch staatliche Maßnahmen zur Überwachung derzeit stark ausgebaut und müssen von Providern unterstützt werden. Nicht immer sind die vorgesehenen Maßnahmen rechtlich unbedenklich.

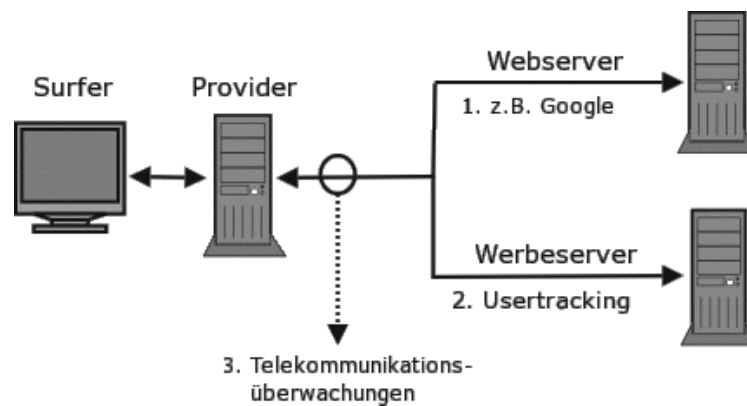


Abbildung 1: Möglichkeiten zur Überwachung im WWW

2 Beispiel Google

Das Beispiel Google wurde aufgrund der Bekanntheit gewählt. Auch andere Firmen gehören zu den *Big Data Companies* und versuchen mit ähnlichen Geschäftsmodellen Gewinne zu erzielen (Facebook, Twitter, MSN, Yahoo, Amazon...).

Viele Nutzer dieser Dienste sehen sich in der Rolle von *Kunden*. Das ist falsch. Kunde ist der, der bezahlt. Kommerzielle Unternehmen optimieren ihre Webangebote, um den zahlenden Kunden zu gefallen und den Gewinn zu maximieren.

Google Web Search

Googles Websuche ist in Deutschland die Nummer Eins. 89% der Suchanfragen gehen direkt an *google.de*. Mit den Suchdiensten wie Ixquick, Metager2, Web.de... die indirekt Anfragen an Google weiterleiten, beantwortet der Primus ca. 95% der deutschen Suchanfragen. (Stand 2008)

1. Laut Einschätzung der Electronic Frontier Foundation werden alle Suchanfragen protokolliert und die meisten durch Cookies, IP-Adressen und Informationen von Google Accounts einzelnen Nutzern zugeordnet.

In den Datenschutzbestimmungen von Google kann man nachlesen, dass diese Informationen (in anonymisierter Form) auch an Dritte weitergegeben werden. Eine Einwilligung der Nutzer in die Datenweitergabe liegt nach Ansicht der Verantwortlichen vor, da mit der Nutzung des Dienstes auch die AGBs akzeptiert wurden. Sie sind schließlich auf der Website öffentlich einsehbar.

2. Nicht nur die Daten der Nutzer werden analysiert. Jede Suchanfrage und die Reaktionen auf die angezeigten Ergebnisse werden protokolliert und ausgewertet.

Google Flu Trends zeigt, wie gut diese Analyse der Suchanfragen bereits arbeitet. Anhand der Such-Protokolle wird eine Ausbreitung der Grippe um 1-2 Wochen schneller erkannt, als es bisher dem U.S. Center for Disease Control and Prevention möglich war.

Die mathematischen Grundlagen für diese Analysen wurden im Rahmen der Bewertung von Googles 20%-Projekten entwickelt. Bis 2008 konnten Entwickler bei Google 20% ihrer Arbeitszeit für eigene Ideen verwenden. Interessante Ansätze aus diesem Umfeld gingen als Beta-Version online (z.B. Orkut). Die Reaktionen der Surfer auf diese Angebote wurde genau beobachtet. Projekte wurden wieder abgeschaltet, wenn sie die harten Erfolgskriterien nicht erfüllten (z.B. Google Video).

Inzwischen hat Google die 20%-Klausel abgeschafft. Die Kreativität der eigenen Mitarbeiter ist nicht mehr notwendig und zu teuer. Diese Änderung der Firmanpolitik wird von iner Fluktuation des Personals begleitet. 30% des kreativen Stammpersonals von 2000 haben der Firma inzwischen den Rücken zugekehrt. (Stand 2008)

Die entwickelten Bewertungsverfahren werden zur Beobachtung der Trends im Web eingesetzt. Der Primus unter den Suchmaschinen ist damit in der Lage, erfolgversprechende Ideen und Angebote schneller als alle Anderen zu erkennen und darauf zu reagieren. Die Ideen werden nicht mehr selbst entwickelt, sondern aufgekauft und in das Imperium integriert. Seit 2004 wurden 60 Firmen übernommen, welche zuvor die Basis für die meisten aktuellen Angebote von Google entwickelt hatten: Youtube, Google Docs, Google Maps, Google Earth, Google Analytics, Picasa, SketchUp, die Blogger-Plattformen...

Das weitere Wachstum des Imperiums scheint langfristig gesichert.

Zu spät hat die Konkurrenz erkannt, welches enorme Potential die Auswertung von Suchanfragen darstellt. Mit dem Börsengang 2004 musste Google seine Geheimniskrämerei etwas lockern und für die Bösenaufsicht Geschäftsdaten veröffentlichen. Microsoft hat daraufhin Milliarden Dollar in *MSN Live Search*, *Bing* versenkt und Amazon, ein weiterer Global Player im Web, der verniedlichend als Online Buchhändler bezeichnet wird, versuchte mit *A9* ebenfalls eine Suchmaschine zu etablieren.

Adsense, DoubleClick, Analytics & Co.

Werbung ist die Haupteinnahmequelle von Google. Im dritten Quartal 2010 erwirtschaftete Google 7,3 Milliarden Dollar und damit 97% der Einnahmen aus Werbung. Zielgenaue Werbung basierend auf umfassenden Informationen über Surfer bringt wesentliche höhere Einkünfte, als einfache Bannerschaltung. Deshalb sammeln Werbetreibende im Netz, umfangreiche Daten über Surfer. Es wird beispielsweise verfolgt, welche Webseiten ein Surfer besucht und daraus ein Interessenprofil abgeleitet. Die Browser werden mit geeigneten Mitteln

markiert (Cookies u.ä.), um Nutzer leichter wieder zu erkennen.

Inzwischen lehnen 84% der Internetnutzer dieses Behavioral Tracking ab. Von den Unternehmen im Internet wird es aber stetig ausgebaut. Google ist auf diesem Gebiet führend und wird dabei (unwissentlich?) von vielen Website-Betreibern unterstützt.

97% der TOP100 Websites und ca. 80% der deutschsprachigen Webangebote sind mit verschiedenen Elementen von Google für die Einblendung kontextsensitiver Werbung und Traffic-Analyse infiziert! (Reppesgaard: Das Google Imperium, 2008) Jeder Aufruf einer derart präparierten Website wird bei Google registriert, ausgewertet und einem Surfer zugeordnet.

Neben kommerziellen Verkaufs-Websites, Informationsangeboten professioneller Journalisten und Online-Redaktionen gehören die Websites politischer Parteien genauso dazu, wie unabhängige Blogger auf den Plattformen *blogger.com* und *blogspot.com* sowie private Websites, die sich über ein paar Groschen aus dem AdSense-Werbe-Programm freuen.

Untragbar wird diese Datenspionage, wenn politische Parteien wie die CSU ihre Spender überwachen lassen. Die CSU bietet ausschließlich die Möglichkeit, via Paypal zu spenden. Die Daten stehen damit inklusive Wohnanschrift und Kontonummer einem amerikanischen Großunternehmen zur Verfügung. Außerdem lässt die CSU ihre Spender mit Google-Analytics beobachten. Der Datenkrake erhält damit eindeutige Informationen über politischen Anschauungen. Diese Details können im Informationskrieg wichtig sein.

Damit kennt das Imperium nicht nur den Inhalt der Websites, die vom Google-Bot für den Index der Suchmaschine abgeklappert wurden. Auch Traffic und Besucher der meisten Websites sind bekannt. Diese Daten werden Werbetreibenden anonymisiert zur Verfügung gestellt.

Die Grafik Bild 2 zur Besucherstatistik wurde vom Google Ad-Planner für eine (hier nicht genannte) Website erstellt. Man erkennt, dass der überwiegende Anteil der Besucher männlich und zwischen 35-44 Jahre alt ist. (Die Informationen zu Bildung und Haushaltseinkommen müssen im Vergleich zu allgm. Statistiken der Bevölkerung bewertet werden, was hier mal entfällt.)

Wie kommt das Imperium zu diesen Daten? Es gibt so gut wie keine Möglichkeit, diese Daten irgendwo einzugeben. Google fragt NICHT nach diesen Daten, sie werden aus der Analyse des Surf- und Suchverhaltens gewonnen. Zusätzlich kauft Google bei Marktforschungsunternehmen große Mengen an Informationen, die in die Kalkulation einfließen.

Wenn jemand mit dem iPhone auf der Website von BMW die Preise von Neuwagen studiert, kann Google ihn einer Einkommensgruppe zuordnen. Wird der Surfer später beim Besuch von Spiegel-Online durch Einblendung von Werbung wiedererkannt, kommt ein entsprechender Vermerk in die Datenbank. Außerdem kann die Werbung passend zu seinen Interessen und Finanzen präsentiert werden. (Die Realität ist natürlich etwas komplexer.)

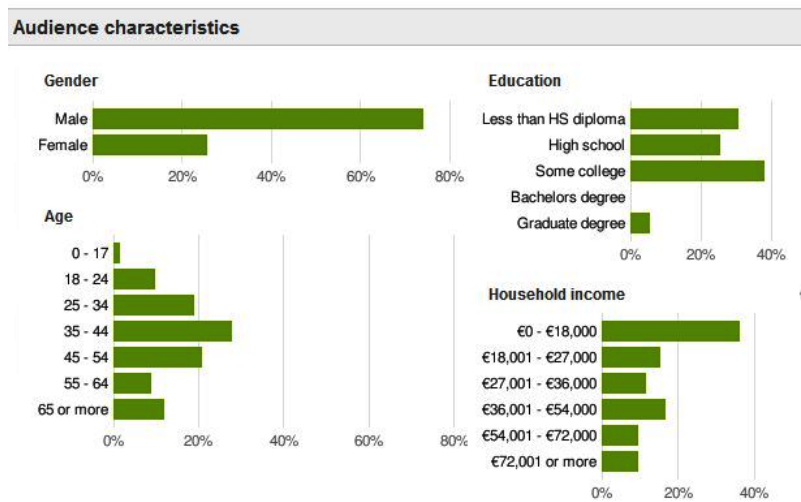


Abbildung 2: Ad-Planner Besucherstatistik (Beispiel)

Mit dem im April 2010 eingeführtem **Retargeting** geht Google noch weiter. Mit Hilfe spezieller Cookies werden detaillierte Informationen über Surfer gesammelt. Die Informationen sollen sehr genau sein, bis hin zu Bekleidungsgrößen, für die man sich in einem Webshop interessiert hat. Die gesammelten Informationen sollen die Basis für punktgenaue Werbung bieten. Beispielsweise soll nach dem Besuch eines Webshops für Bekleidung ohne Kaufabschluss permanent alternative Werbung zu diesem Thema eingeblendet werden.

Google Mail, Talk, News... und Google+ (personalisierte Dienste)

Mit einem einheitlichem Google-Konto können verschiedene personalisierte Angebote genutzt werden. (Google Mail, News, Talk, Calendar, Alert, Orkut, Börsennachrichten..... iGoogle)

Bei der Anmeldung ist das Imperium weniger wissbegierig, als vergleichbare kommerzielle Anbieter. Vor- und Nachname, Login-Name und Passwort reichen aus. Es ist nicht unbedingt nötig, seinen realen Namen anzugeben. Ein Pseudonym wird auch akzeptiert. Die Accounts ermöglichen es, aus dem Surf- und Suchverhalten, den zusammengestellten Nachrichtenquellen, dem Inhalt der E-Mails usw. ein Profil zu erstellen. Die unsicher Zuordnung über allgemeine Cookies, IP-Adressen und andere Merkmale ist nicht nötig.

Außerdem dienen die Dienste als Flächen für personalisierte und gut bezahlte Werbung.

Patente aus dem Umfeld von Google Mail zeigen, dass dabei nicht nur Profile über die Inhaber der Accounts erstellt werden, sondern auch die Kommunikationspartner unter die Lupe genommen werden. Wer an einen

Google Mail Account eine eMail sendet, landet in der Falle des Datenkraken.

Die Einrichtung eines Google-Accounts ermöglicht es aber auch, gezielt die gesammelten Daten in gewissem Umfang zu beeinflussen. Man kann Einträge aus der Such- und Surf-Historie löschen u.ä. (Besser ist es sicher, die Einträge von vornherein zu vermeiden.)

Smartphones und Android

2005 hat Google die Firma Android Inc. für 50 Mio. Dollar gekauft sucht mit dem Smartphone Betriebssystem Android auf dem Markt der mobilen Kommunikation ähnliche Erfolge wie im Web.

Das erste Google Handy *G1* war ein in Hardware gegossenes Pendant zum Webbrowser Google Chrome. Bei der Markteinführung versuchte Google die Nutzer mit dem ersten Einschalten zu überreden, einen Google-Account anzulegen. Ohne Account bei Google ging fast nichts mit dem Hightech-Spielzeug, nur Telefonieren war möglich. Dieses Feature wurde auf Druck der Nutzer deaktiviert.

Bei der Nutzung von Android Smartphones sollen alle E-Mails über Google Mail laufen, Termine mit dem Google Calendar abgeglichen werden, die Kontaktdaten sollen bei Google landen. . . Die Standortdaten werden ständig an Google übertragen, um sogenannte Mehrwertdienste bereit zu stellen (genau wie das iPhone die Standortdaten an Apple sendet).

Inzwischen ist die feste Bindung an Google-Dienste unter Android etwas gelockert. Aber nach wie vor sind diese als Standard voreingestellt und werden aus Bequemlichkeit sicher von der Mehrzahl der Nutzer verwendet.

Mozilla Firefox

Google ist der Hauptsponsor der Firefox Entwickler. Seit 2012 zahlt Google jährlich 300 Mio. Dollar an die Mozilla Foundation, um die Standardsuchmaschine zu sein.

Das ist natürlich in erster Linie ein Angriff auf Microsoft, den dominierenden Internet Explorer und die Suchmaschine Bing. Die Entwickler von Firefox kommen ihrem datensammelnden Hauptsponsor jedoch in vielen Punkten deutlich entgegen:

- Google ist die einzige allgemeine Suchmaschine, die unbedarften Nutzern zur Verfügung steht. Alternativen sind standardmäßig nicht vorhanden und müssen von den Nutzer aktiv gesucht und installiert werden.
- Die Default-Startseite ermöglicht es Google, ein langlebiges Cookie zu setzen und den Browser damit praktisch zu personalisieren.
- Sollte die Startseite modifiziert werden (z.B. bei der Variante *Iceweasel* von Debian GNU/Linux), erfolgt die "Personalisierung" des Browsers wenige Minuten später durch Aktualisierung der Phishing-Datenbank.

- Diese “Personalisierung” ermöglicht es Google, den Nutzer auf allen Webseiten zu erkennen, die mit Werbeanzeigen aus dem Imperium oder Google-Analytics verschmutzt sind. Im deutschsprachigen Web hat sich diese Verschmutzung auf 4/5 der relevanten Webseiten ausgebreitet.

(Trotzdem ist Mozilla Firefox ein guter Browser. Mit wenigen Anpassungen und Erweiterungen von unabhängigen Entwicklern kann man ihm die Macken austreiben und spurenarm durchs Web surfen.)

Google DNS

Mit dem DNS-Service versucht Google, die Digital Natives zu erreichen, Surfer die in der Lage sind, Cookies zu blockieren, Werbung auszublenden und die natürlich einen DNS-Server konfigurieren können.

Google verspricht, dass die DNS-Server unter den IP-Adressen 8.8.8.8 und 8.8.4.4 nicht kompromittiert oder zensiert werden und bemüht sich erfolgreiche um schnelle DNS-Antworten. Die Google-Server sind etwa 1/10 sec bis 1/100 sec schneller als andere unzensierte DNS-Server.

Natürlich werden alle Anfragen gespeichert und ausgewertet. Ziel ist, die von erfahrenen Nutzern besuchten Websites zu erfassen und in das Monitoring des Web besser einzubeziehen. Positiv an dieser Initiative von ist, dass es sich kaum jemand leisten kann, die Wirtschaftsmacht Google zu blockieren. Damit wird auch die Sperrung alternativer DNS-Server, wie es in Deutschland im Rahmen der Einführung der Zensur geplant war, etwas erschwert.

Kooperation mit Behörden und Geheimdiensten

Es wäre verwunderlich, wenn die gesammelten Datenbestände nicht das Interesse der Behörden und Geheimdienste wecken würden. Google kooperiert auf zwei Ebenen:

1. Auf Anfrage stellt Google den Behörden der Länder die angeforderten Daten zur Verfügung. Dabei agiert Google auf Grundlage der nationalen Gesetze. Bei daten-speicherung.de findet man Zahlen zur Kooperationswilligkeit des Imperiums. Durchschnittlich beantwortet Google Anfragen mit folgender Häufigkeit:
 - 3mal täglich von deutschen Stellen
 - 20mal täglich von US-amerikanischen Stellen
 - 6mal täglich von britischen Stellen
2. Außerdem kooperiert Google mit der CIA bei der Auswertung der Datenbestände im Rahmen des Projektes *Future of Web Monitoring*, um Trends und Gruppen zu erkennen und für die Geheimdienste der USA zu erschließen. Es besteht der Verdacht, dass Google auch mit der NSA kooperiert. Das EPIC bemüht sich, Licht in diese Kooperation zu bringen. Anfragen wurden bisher nicht beantwortet.

Die (virtuelle) Welt ist eine "Google" - oder?

Die vernetzten Rechenzentren von Google bilden den mit Abstand größten Supercomputer der Welt. Dieser Superrechner taucht in keiner TOP500-Liste auf, es gibt kaum Daten, da das Imperium sich bemüht, diese Informationen geheim zu halten. Die Datenzentren werden von (selbständigen?) Gesellschaften wie Exaflop LLC betrieben.

Neugierige Journalisten, Blogger und Technologieanalysten tragen laufend neues Material über diese Maschine zusammen. In den Materialsammlungen findet man 12 bedeutende Anlagen in den USA und 5 in Europa, die als wesentliche Knotenpunkte des Datenuniversums eingeschätzt werden. Weitere kleinere Rechenzentren stehen in Dublin, Paris, Mailand, Berlin, München Frankfurt und Zürich. In Council Bluffs (USA), Thailand, Malaysia und Litauen werden neue Rechenzentren gebaut, die dem Imperium zuzurechnen sind. Das größte aktuelle Bauprojekt vermuten Journalisten in Indien. (2008)

Experten schätzen, dass ca. 1 Mio. PCs in den Rechenzentren für Google laufen (Stand 2007). Alle drei Monate kommen etwa 100 000 weitere PCs hinzu. Es werden billige Standard-Komponenten verwendet, die zu Clustern zusammengefasst und global mit dem *Google File System (GFS)* vernetzt werden. Das GFS gewährleistet dreifache Redundanz bei der Datenspeicherung.

Die Kosten für diese Infrastruktur belaufen sich auf mehr als zwei Milliarden Dollar jährlich. (2007)

Die Videos von Youtube sollen für 10% des gesamten Traffics im Internet verantwortlich sein. Über den Anteil aller Dienste des Imperiums am Internet-Traffic kann man nur spekulieren.

Google dominiert unser (virtuelles) Leben.

Dabei geht es nicht um ein paar Cookies sondern um eine riesige Maschinerie.

Das Image ist (fast) alles

Die Achillesferse von Google ist das Image. In Ländern, die traditionell skeptisch gegenüber amerikanischen Unternehmen eingestellt sind, konnte Google längst nicht diese Markbeherrschung aufbauen wie in den USA und Westeuropa.

In Russland und China beantwortet der Suchdienst weniger als 20% der Anfragen. Primus in Russland ist die Suchmaschine *Yandex*, in China dominiert *Baidu*, in Tschechien *Seznam*.

3 User-Tracking

Viele Dienste im Web nutzen die Möglichkeiten, das Surfverhalten zu verfolgen, zu analysieren und die gesammelten Daten zu versilbern. Die dabei entstehenden Nutzerprofile sind inzwischen sehr aussagekräftig. Wie das Wall Street Journal in einer Analyse beschreibt, können das Einkommen, Alter, politische Orientierung und weitere persönliche Daten der Surfer eingeschätzt werden

oder die Wahrscheinlichkeit einer Kreditrückzahlung. Hauptsächlich werden diese Daten für Werbung genutzt. Ein Onlin-Versand von Brautkleidern möchte Frauen im Alter von 24-30 Jahren ansprechen, die verlobt sind. Das ist heute möglich.

Eine weitere Analyse des Wall Street Journal nimmt die Firma Rapleaf näher unter die Lupe. Diese Firma ist auf die Auswertung von Cookies spezialisiert. Neben den genannten Persönlichkeitsprofilen kann Rapleaf auch den realen Namen und viele genutzte E-Mail Adressen aufdecken. Diese Informationen werden meist durch Nutzung von Facebook o.ä verraten.

Häufig werden *Werbeeinblendungen* für das User-Tracking genutzt. Die in Webseiten dargestellte Werbung wird nur von wenigen Anbietern zur Verfügung gestellt. Diese verwenden verschiedene Möglichkeiten, um Surfer zu erkennen, das Surfverhalten Website übergreifend zu erfassen und anhand dieser Daten Nutzerprofile zu generieren. Für die Auswertung werden nicht nur die besuchten Websites genutzt. Besonders aussagekräftig sind die Klicks auf Werbung. S. Guha von Microsoft und B. Cheng sowie P. Francis vom Max Planck Institute für Software Systeme beschreiben in einer wiss. Veröffentlichung, wie man homosexuelle Männer anhand der Klicks auf Werbung erkennen kann. Das Verfahren kann für verschiedene Fragestellungen angepasst werden.

Neben Werbung und Cookies werden auch *HTML-Wanzen* (so genannten *Webbugs*) für das Tracking eingesetzt. Dabei handelt es sich um 1x1-Pixel große transparente Bildchen, welche in den HTML-Code einer Webseite oder einer E-Mail eingebettet werden. Sie sind für den Nutzer unsichtbar, werden beim Betrachten einer Webseite oder Öffnen der E-Mail vom externen Server geladen und hinterlassen in den Logs des Servers Spuren für eine Verfolgung des Surfverhaltens.

Außerdem gibt es spezielle Tracking-Dienste wie Google Analytics, die oft mit Javascript arbeiten.

Gesetzliche Schranken scheint man großflächig zu ignorieren. Die Universität Karlsruhe hat eine Studie veröffentlicht, die zu dem Ergebnis kommt, dass nur 5 von 100 Unternehmen im Internet geltende Gesetze zum Datenschutz respektieren. Der Nutzer ist also auf Selbstschutz angewiesen.

Tracking von Dokumenten

Die Firma ReadNotify bietet einen Service, der E-Mails, Office-Dokumente und PDF-Dateien mit speziellen unsichtbaren Elementen versieht. Diese werden beim Öffnen einer E-Mail oder eines Dokuments vom Server der Firma nachgeladen und erlauben somit eine Kontrolle, wer wann welches Dokument öffnet. Via Geo-Location ermittelt ReadNotify auch den ungefähren Standort des Lesers.

Die Markierung von E-Mail Newslettern ist relativ weit verbreitet, aber nicht immer legal. Es wird nicht nur im kommerziellen Bereich verwendet. Auch die CDU Brandenburg markierte ihre Newsletter über einen längeren Zeitraum, um

zu überprüfen, wann und wo sie gelesen wurden.

Nutzen der Informationen für Angriffe

Neben der unerwünschten Protokollierung der Daten besteht die Gefahr, dass böswillige Betreiber von Websites die Informationen über die verwendeten Versionen der Software gezielt ausnutzen, um mittels bekannter Exploits (Sicherheitslücken) Schadensroutinen einzuschleusen und damit die Kontrolle über den Rechner zu erlangen.

Derartig übernommene Rechner werden häufig als Spamschleuder missbraucht oder nach sensiblen Informationen (z.B. Kontodaten) durchsucht. Es sind auch gezielte Anwendungen zur Spionage bekannt. Das von chinesischen Hackern mit manipulierten PDF-Dokumenten aufgebaute Ghostnet konnte 2008 erfolgreich die Computersysteme von westlichen Regierungen und des Dalai Lama infizieren. Eine Analyse des Kontrollzentrums Ghost RAT zeigte die umfangreichen Möglichkeiten der Malware. Es konnten Keylogger installiert werden, um an Bankdaten und Passwörter zu gelangen, das Mikrofon konnte für die Raumüberwachung genutzt werden.....

4 History Sniffing

Die aktuellen Browser speichern Informationen über besuchte Webseiten in einer History.

Eine empirische Untersuchung der University of California zeigt, dass ca. 1% der Top 50.000 Websites versuchen, diese Daten über zuvor besuchte Websites auszulesen. Daneben gibt es spezielle Anbieter wie Tealium oder Beencounter, die einem kleineren Webmaster in Echtzeit eine Liste der Websites liefern, die ein Surfer zuvor besucht hat.

Die dabei übermittelten Informationen erlauben ein ähnlich detailliertes Interessenprofil zu erstellen, wie das User Tracking über viele Websites. Ein Experiment des Isec Forschungslabors für IT-Sicherheit zeigt, dass diese History-Daten zur Deanonymisierung der Surfer genutzt werden können. Anhand der Browser History wurde ermittelt, welche Gruppen bei Xing der Surfer bisher besucht hat. Da es kaum zwei Nutzer gibt, die zu den gleichen Gruppen gehören, konnte mit diesen Daten eine Deanonymisierung erfolgen. Die Realnamen sowie E-Mail Adressen wurden ohne Mithilfe des Surfer nur durch den Aufruf der präparierten Webseite ermittelt.

In der Regel wird obfuscated Javascript Code für den Angriff genutzt. Die Websites werden bewusst so gestaltet, dass sie ohne Javascript nicht benutzbar sind, um eine Deaktivierung von Javascript zu verhindern. Außerdem können für moderne Browser CSS-Hacks für das History-Sniffing verwendet werden.

Die derzeit einzig wirksame Verteidigung gegen diesen Angriff besteht in der Deaktivierung der Browser History.

5 Geotagging

Geotagging ist *the next big thing* unter den Angriffen auf die Privatsphäre. Es geht um die Frage, wo wir etwas tun oder getan haben und welche Bewegungsmuster erkennbar sind.

1. **Standortdaten** sind die wertvollsten Informationen für die Werbewirtschaft, um zukünftig den Markt zu vergrößern. Ein Online-Versand von Brautkleidern richtet seine Werbung an Frauen zwischen 24-30 Jahren, die verlobt sind. Ein Ladengeschäft stellt zusätzlich die Bedingung, dass sie sich häufig im Umkreis von xx aufhalten. Gezielte lokalisierte Werbung ist ein Markt, der durch die Verbreitung von Smartphones stark wächst.
2. Die **Bewegungsanalyse** ermöglicht Aussagen über sehr private Details. Man kann z.B. durch die Analyse der Handybewegungen erkennen, ob jemand als Geschäftsreisender häufig unterwegs ist, ob man ein festes Arbeitsverhältnis hat, für welche Firma man tätig ist oder ob man arbeitslos ist. Die Firma Sense Networks ist ein Vorreiter auf dem Gebiet der Bewegungsanalyse. Im Interview mit *Technology Review* beschreibt Greg Skibiski seine Vision:

Es entsteht ein fast vollständiges Modell. Mit der Beobachtung dieser Signale kann man ganze Firmen, ganze Städte, eine ganze Gesellschaft röntgen.

<http://www.heise.de/tr/artikel/Immer-im-Visier-276659.html>

Das Magazin Wired berichtete im Danger Room (Oktober 2011), dass das FBI Smartphones bereits seit Jahren mit dieser Zielstellung der "Durchleuchtung der Gesellschaft" traktiert. Muslimische Communities werden systematisch analysiert, ohne dass die betroffenen Personen im Verdacht einer Straftat stehen. Das Geotracking von GPS-fähigen Smartphones und GPS-Modulen moderner Fahrzeuge durch das FBI erfolgt ohne richterlichen Beschluss.

... the pushpins on the new FBI geo-maps indicate where people live, work, pray, eat and shop, not necessarily where they commit or plan crimes.

<http://www.wired.com/dangerroom/2011/10/fbi-geomaps-muslims>

Datensammlung

Die Daten werden mit verschiedenen Methoden gesammelt:

- Hauptlieferanten für Geodaten sind Smartphones und Handys. Vor allem Apps können genutzt werden, um Geodaten zu sammeln. Über die Hälfte der in verschiedenen Stores downloadbaren Apps versenden Standortdaten unabhängig davon, ob sie für die Funktion der App nötig sind. Der Bundesdatenschutzbeauftragte erwähnt beispielsweise eine App, die das Smartphone zur Taschenlampe macht und dabei den Standort an

den Entwickler der App sendet.

- Mit Einführung des iPhone 4 hat Apple seine Datenschutzbestimmungen geändert. Die gesamte Produktpalette von Apple (iPhone, Laptops, PC...) wird in Zukunft den Standort des Nutzers laufend an Apple senden. Apple wird diese Daten Dritten zur Verfügung stellen. Wer Zugang zu diesen Daten hat, wird nicht näher spezifiziert. <http://www.apple.com/chde/legal/privacy/>

Für die Datensammlungen rund um das iPhone wurde Apple mit dem Big-Brother Award 2011 geehrt. Auszug aus der Laudation von F. Rosengart und A. Bogk:

Apples Firmenstrategie scheint darauf ausgelegt zu sein, möglichst viele Daten der Nutzer zu erfassen, ähnlich wie es soziale Netzwerke auch tun. Werbepartner freuen sich darauf, mit Hilfe von Apple möglichst zielgruppengerechte und standortbezogene Werbung auf dem Telefon anzeigen zu können.

- Millionen von Fotos werden über verschiedene Dienste im Internet veröffentlicht (Flickr, Twitter, Facebook...). Häufig enthalten diese Fotos in den EXIF-Attributen die GPS-Koordinaten der Aufnahme. Die Auswertung dieses Datenstromes steht erst am Anfang der Entwicklung. Ein Beispiel ist die Firma Heypic, die mit Risikokapital ausgestattet die Fotos von Twitter durchsucht und auf einer Karte darstellt.
- Die ganz normale HTTP-Kommunikation liefert Standortinformationen anhand der IP-Adresse. Aktuelle Browser bieten zusätzlich eine Geolocation-API, die genauere Informationen zur Verfügung stellt. Als Facebook im Sommer 2010 die Funktion Places standardmäßig aktivierte, waren viele Nutzer überrascht, wie genau jede reale Bewegung im Sozialen Netz lokalisiert wird. (Nicht nur Facebook kann das.)



Abbildung 3: Lokalisierung eines Smartphone durch Facebook

Die Deaktivierung von Places scheint bei Facebook wirklich umständlich zu sein. Damit wird aber nicht die Erfassung der Daten deaktiviert, sondern nur die Sichtbarkeit für andere Nutzer!

- Lokalisierungsdienste wie *Gowalla* oder *Foursquare* bieten öffentlich einsehbare Standortdaten und versuchen, durch spielartigen Charakter neue Nutzer zu gewinnen. Im Gegensatz zu den oben genannten Datensammlungen kann man bei Gowalla oder Foursquare aber gut kontrollieren, welche Daten man veröffentlicht oder die Dienste nicht nutzen.

Nichts zu verbergen?

Wer ein praktisches Beispiel braucht: Einer Kanadierin wurde das Krankengeld gestrichen, weil sie auf Facebook fröhliche Urlaubsfotos veröffentlichte. Die junge Frau war wegen Depressionen krank geschrieben und folgte dem Rat ihres Arztes, einmal Urlaub zu machen und Zusammenkünfte mit Freunden zu suchen. Die Krankenkasse nutze keine technischen Geo-Informationen sondern stellte visuell durch Beobachtung des Facebook-Profiles den Aufenthaltsort fest. Aber das Beispiel zeigt, dass die automatisierte Auswertung Konsequenzen haben könnte. <http://www.magnus.de/news/krankengeld-gestrichen-wegen-verfaenglichen-facebook-bildern-208271.html>

6 Kommunikationsanalyse

Geheimdienste verwenden seit Jahren die Kommunikations-Analyse (wer mit wem kommuniziert), um die Struktur von Organisationen aufzudecken. Teilweise gelingt es damit, die Verschlüsselung von Inhalten der Kommunikation auszuhebeln und umfangreiche Informationen zu beschaffen.

Auch ohne Kenntnis der Gesprächs- oder Nachrichteninhalte - die nur durch Hineinhören zu erlangen wäre - lässt sich allein aus dem zeitlichen Kontext und der Reihenfolge des Kommunikationsflusses eine hohe Informationsgüte extrahieren, nahezu vollautomatisch.
(Frank Rieger)

Die Verwendung der Daten demonstriert das **Projekt Gegenwirken** der niederländischen Geheimdienste. In regierungskritischen Organisationen werden die Aktivisten identifiziert, deren Engagement für die Gruppe wesentlich ist. Für die Kommunikationsanalyse nötigen Daten werden dabei u.a. mit systematisch illegalen Zugriffen gewonnen. Die identifizierten Aktivisten werden mit kleinen Schikanen beschäftigt um die Arbeit der Gruppe zu schwächen. Das Spektrum reicht von ständigen Steuerprüfungen bis zu Hausdurchsuchungen bei harmlosen Bagatelldelikten.

Zivile Kommunikations-Analyse

Zunehmend wird auch im zivilen Bereich diese Analyse eingesetzt. Das Ziel ist es, Meinungsmacher und kreative Köpfe in Gruppen zu identifizieren, gezielt mit Werbung anzusprechen und sie zu manipulieren. Im Gegensatz zu den Diensten haben Unternehmen meist keinen Zugriff auf Verbindungsdaten von Telefon und Mail. Es werden öffentlich zugängliche Daten gesammelt.

Die Freundschaftsbeziehungen in sozialen Netzen wie Facebook oder ...VZ werden analysiert. Ehemalige Studenten des MIT demonstrierten mit Gaydar -

die Schulfalle, wie man homosexuelle Orientierung einer Person anhand ihrer Freundschaftsbeziehungen erkennt. Twitter bietet ein umfangreichen Datenpool oder die Kommentare in Blogs und Foren. Teilweise werden von Unternehmen gezielt Blogs und Foren zu bestimmten Themen aufgesetzt, um Daten zu generieren. In diesen Communitys wird die Position einzelner Mitglieder analysiert, um die Meinungsmacher zu finden.

Gegenwärtig ist die Analyse von Gruppen Gegenstand intensiver Forschung (sowohl im zivilen wie auch geheimdienstlichem Bereich). Die TU Berlin hat zusammen mit der Wirtschaftsuniversität Wien erfolversprechende Ergebnisse zur *Rasterfahndung nach Meinungsmachern* veröffentlicht. Die EU hat mit *INDECT* ein ambitioniertes Forschungsprojekt gestartet, um das Web 2.0 für die Dienste zu erschließen und direkt mit der ständig erweiterten Video-Überwachung zu verbinden.

7 Überwachungen im Internet

Unter <http://www.daten-speicherung.de/index.php/ueberwachungsgesetze> findet man eine umfassende Übersicht zu verschiedene Sicherheits-Gesetzen der letzten Jahre. Neben einer Auflistung der Gesetze wird auch dargestellt, welche Parteien des Bundestages dafür und welche Parteien dagegen gestimmt haben. Sehr schön erkennbar ist das Muster der Zustimmung durch die jeweiligen Regierungsparteien und meist Ablehnung durch die Opposition, von Böswilligen als Demokratie-Simulation bezeichnet. Unabhängig vom Wahlergebnis wird durch die jeweiligen Regierungsparteien die Überwachung ausgebaut, denn **Du bist Terrorist!** (<http://www.dubistterrorist.de>)

Vorratsdatenspeicherung oder Mindest-Speicherfrist Ohne jeglichen Verdacht sollen die Verbindungsdaten jeder E-Mail, jedes Telefonats, jeder SMS und Standortdaten der Handys gesammelt werden.

Die Versuche zur Einführung sind nicht neu. 1997 wurde die VDS aufgrund verfassungsrechtlicher Bedenken abgelehnt, 2002 wurde ein ähnlicher Gesetzentwurf vom Deutschen Bundestag abgelehnt und die Bundesregierung beauftragt, gegen einen entsprechenden Rahmenbeschluss auf EU-Ebene zu stimmen (siehe Bundestag-Drucksache 14/9801). Der Wissenschaftliche Dienst des Bundestages hat bereits 2006 ein Rechtsgutachten mit schweren Bedenken gegen die VDS vorgelegt.

Ein Vergleich der Zahlen der Kriminalitätsstatistik des BKA für die Jahre 2007, 2008 und 2009 zeigt, dass die VDS im Jahr 2009 nicht zur einer Verbesserung der Aufklärungsrate von Straftaten im Internet führte.

	2007 (o. VDS)	2008 (o. VDS)	2009 (mit VDS)
Straftaten im Internet	179.026	167.451	206.909
Aufklärungsrate (Internet)	82.9%	79.8%	75.7

Eine umfangreiche wissenschaftliche Analyse des des Max-Planck-Instituts (MPI) für ausländisches und internationales Strafrecht belegt,

dass KEINE *Schutzlücke* ohne Vorratsdatenspeicherung besteht und widerspricht damit der Darstellung von mehreren Bundesinnenministern und BKA-Chef Ziercke, wonach die VDS für die Kriminalitätsbekämpfung unbedingt nötig wäre. Die in der Presse immer wieder herangezogenen Einzelbeispiele halten einer wissenschaftlichen Analyse nicht stand.

In einem offenen Brief sprachen sich Richter und Staatsanwälte gegen die VDS aus und widersprechen ebenfalls der Notwendigkeit für die Kriminalitätsbekämpfung.

Zensur im Internet Die Zensur sollte in Deutschland im Namen des Kampfes gegen Kinderpornografie im Internet eingeführt werden. Man wurde nicht müde zu behaupten, es gäbe einen Millionen Euro schweren Massenmarkt, der durch Sperren von Websites empfindlich ausgetrocknet werden kann. Die Aussagen wurden überprüft und für falsch befunden. <http://blog.odem.org/2009/05/quellenanalyse.html>

1. In der ersten Stufe unterzeichneten im Frühjahr 2009 die fünf großen Provider freiwillig einen geheimen Vertrag mit dem BKA. Sie verpflichteten sich, eine Liste von Websites zu sperren, die vom BKA ohne nennenswerte Kontrolle erstellt werden sollte.
2. In der zweiten Stufe wurde am 18.06.09 das *Zugangerschwernisgesetz* verabschiedet. Alle Provider mit mehr als 10.000 Kunden sollen diese geheime Liste von Websites zu sperren. Neben den (ungeeigneten) DNS-Sperren sollen auch IP-Sperren und Filterung der Inhalte zum Einsatz kommen.
3. Die CDU/FDP-Regierung ist im Herbst 2009 einen halben Schritt zurück gegangen und hat mit einem Anwendungserlass die Umsetzung des Gesetzes für ein Jahr aufgeschoben. Diese Regierung meint also, über dem Parlament zu stehen und ein beschlossenes Gesetz nicht umsetzen zu müssen.
4. Im Rahmen der Evaluierung des Gesetzes geht das BKA nur halbherzig gegen dokumentierten Missbrauch vor, wie eine Veröffentlichung des AK-Zensur zeigt. Gleichzeitig wird weiter Lobbyarbeit für das Zensurgesetz betrieben. <http://ak-zensur.de/2010/08/kapitulation.html>
5. Die Auswertung des eco Verband zeigt, dass Webseiten mit dokumentiertem Missbrauch effektiv gelöscht werden können. 2010 wurden 99,4% der gemeldeten Webseiten gelöscht. http://www.eco.de/verband/202_8727.htm
6. Im Herbst 2011 wurde das Gesetz offiziell beerdigt.

Der Aufbau einer Infrastruktur für Zensur im Internet wird auf vielen Wegen betrieben. Neben dem Popanz "*Kinderpornografie*" engagiert sich die Content Mafia im Rahmen der geheimen ACTA Verhandlungen für eine verbindliche Verpflichtung zum Aufbau der Infrastruktur für Websperren. Die CDU/CSU Bundestagsfraktion sieht die amerikanischen Gesetzesvorlagen SOPA und PIPA als richtungsweisend an. Beide Gesetzesvorlagen sehen umfangreiche Zensurmaßnahmen zum Schutz geistigen

Eigentums vor.

Die verfassungsrechtlichen Bedenken gegen die Zensur hat der wissenschaftliche Dienst des Bundestages in einem Gutachten zusammengefasst. (http://netzpolitik.org/wp-upload/bundestag_filter-gutachten.pdf) Auch eine Abschätzung der EU-Kommission kommt zu dem Schluss, dass diese Sperrmaßnahmen **notwendigerweise eine Einschränkung der Menschenrechte voraussetzen**, beispielsweise der freien Meinungsäußerung.

BKA Gesetz Mit dem BKA Gesetz wird eine Polizei mit den Kompetenzen eines Geheimdienstes geschaffen. Zu diesen Kompetenzen gehören neben der heimlichen Online-Durchsuchung von Computern der Lauschangriff außerhalb und innerhalb der Wohnung (incl. Video), Raster- und Schleierfahndung, weitgehende Abhörbefugnisse, Einsatz von V-Leuten, verdeckten Ermittlern und informellen Mitarbeitern...

Im Rahmen präventiver Ermittlungen (d.h. ohne konkreten Tatverdacht) soll das BKA die Berechtigung erhalten, in eigener Regie zu handeln und Abhörmaßnahmen auch auf Geistliche, Abgeordnete, Journalisten und Strafverteidiger auszudehnen. Im Rahmen dieser Vorfeldermittlungen unterliegt das BKA nicht der Leitungsbefugnis der Staatsanwaltschaft.

Damit wird sich das BKA bis zu einem gewissen Grad jeglicher Kontrolle, der justiziellen und erst recht der parlamentarischen, entziehen können.
Wolfgang Wieland (Grüne)

Telekommunikationsüberwachungsverordnung Auf richterliche Anordnung wird eine Kopie der gesamten Kommunikation an Strafverfolgungsbehörden weitergeleitet. Dieser Eingriff in das verfassungsmäßig garantierte Recht auf unbeobachtete Kommunikation ist nicht nur bei Verdacht schwerer Verbrechen möglich, sondern auch bei einigen mit Geldstrafe bewährten Vergehen und sogar bei Fahrlässigkeitsdelikten (siehe §100a StPO).

Laut Gesetz kann die Überwachung auch ohne richterliche Genehmigung begonnen werden. Sie ist jedoch spätestens nach 3 Tagen einzustellen, wenn bis dahin keine richterliche Genehmigung vorliegt.

Präventiv-polizeil. Telekommunikationsüberwachung ermöglicht es den Strafverfolgungsbehörden der Länder Bayern, Thüringen, Niedersachsen, Hessen und Rheinland-Pfalz den Telefon- und E-Mail-Verkehr von Menschen mitzuschneiden, die keiner(!) Straftat verdächtigt werden. Es reicht aus, in der Nähe eines Verdächtigten zu wohnen oder möglicherweise in Kontakt mit ihm zu stehen.

Die Anzahl der von dieser Maßnahme Betroffenen verdoppelt sich Jahr für Jahr. Gleichzeitig führen nur 17% der Überwachungen zu Ergebnissen im Rahmen der Ermittlungen.

Datenbanken Begleitet werden diese Polizei-Gesetze vom Aufbau umfangreicher staatlicher Datensammlungen. Von der Schwarze Liste der Ausländerfreunde (Einlader-Datei) bis zur AntiTerrorDatei, die bereits 20.000 Personen enthält, obwohl es in Deutschland keinen Terroranschlag gibt. (Abgesehen von den Muppets aus dem Sauerland, deren Islamische Jihad Union offensichtlich eine Erfindung der Geheimdienste ist.)

Elektronischer PA Mit dem Elektronischen Personalausweis wird die biometrische Voll-Erfassung der Bevölkerung voran getrieben. Außerdem werden die Grundlagen für eine eindeutige Identifizierung im Internet gelegt, begleitet von fragwürdigen Projekten wie De-Mail.

Der Elektronische Polizeistaat

Was unterscheidet einen elektronischen Polizeistaat von einer Diktatur? Gibt es dort auch eine Geheime Bundespolizei, die Leute nachts aus der Wohnung holt und abtransportiert, ohne juristischen Verfahren einsperrt...

Ein elektronischer Polizeistaat arbeitet sauberer. Es werden elektronische Technologien genutzt um forensische Beweise gegen BürgerInnen aufzuzeichnen, zu organisieren, zu suchen und zu verteilen. Die Informationen werden unbemerkt und umfassend gesammelt, um sie bei Bedarf für ein juristisches Verfahren als Beweise aufzubereiten.

Würde man noch den Mut haben, gegen die Regierung zu opponieren, wenn diese Einblick in jede Email, in jede besuchte Porno-Website, jeden Telefonanruf und jede Überweisung hat?

Bei einem Vergleich von 52 Staaten hinsichtlich des Ausbaus des elektronischen Polizeistaat hat Deutschland einen beachtlichen 10 Platz belegt. Es verwundert nicht, dass an erster Stelle China und Nordkorea, gefolgt von Weißrussland und Russland stehen. Dann aber wird bereits Großbritannien aufgelistet, gefolgt von den USA, Singapur, Israel, Frankreich und Deutschland.

Noch sei der Polizeistaat nicht umfassen realisiert, "aber alle Fundamente sind gelegt". Es sei schon zu spät, dies zu verhindern. Mit dem Bericht wolle man die Menschen darauf aufmerksam machen, dass ihre Freiheit bedroht ist.

Das dieser Polizeistaat bereits arbeitsfähig ist, zeigt die Affäre Jörg Tauss. Ein unbequemer Politiker mit viel zu engen Kontakten zum CCC, der Datenschutz ernst nimmt, gegen das BKA-Gesetz und gegen Zensur auftritt, wird wenige Monate vor der Wahl des Konsums von KiPo verdächtigt. Die Medien stürzen sich auf das Thema. Innerhalb kurzer Zeit war Tauss als Politiker von der Springer-Presse demontiert, unabhängig von einer Verurteilung.

Ähnliche Meldungen hatten in den letzten Jahren viel weniger Resonanz in der Presse:

1. *Auf dem Dienstcomputer eines hochrangigen Mitglieds des hessischen Innenministeriums sind vermutlich Kinderpornos entdeckt worden. (25.07.2007)*

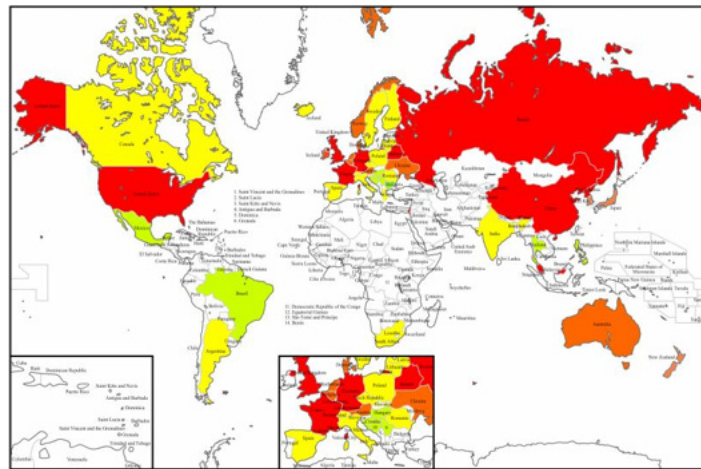


Abbildung 4: Vergleich der elektronischen Polizeistaaten

2. *Kinderpornos: CDU-Politiker unter Verdacht* (01.04.2005)
3. *Der CDU-Politiker Andreas Zwickl aus Neckarsulm ist wegen Verdachts des Besitzes von...* (05.03.2009)

Der Springer-Pressen standen im Fall Tauss umfangreiche Informationen zur Verfügung. Woher kamen diese Informationen? Jemand hat die Ermittlungsakten an die Presse weitergegeben! <http://blog.fefe.de/?ts=b74d1e08>

8 Rechtsstaatliche Grundlagen

Es ist erkennbar, wohin die Reise gehen soll. Die Räder rollen bereits. Es wird Zeit, ein neues Ziel zu buchen, bevor der Zug endgültig abgefahren ist.

Das Post- und Fernmeldegeheimnis, die Unverletzlichkeit der Privatsphäre und der ungehinderte Zugang zu Informationen sind in der UN-Resolution 217 A (III) [5] als grundlegende Menschenrechte definiert. Diese Resolution wurde 1948 unmittelbar nach den Erfahrungen der Diktatur verabschiedet und hat unser Grundgesetz maßgeblich beeinflusst.

Eine verfassungskonforme Gesetzgebung müsste den Intentionen des Grundgesetzes folgen und die in den Artikeln 2, 10 und 13 definierten Grundrechte anerkennen.

1. Ein Eingriff in die vom Grundgesetz geschützten Rechte ist nur zur Verfolgung schwerer Verbrechen zulässig. Es sind vom Gesetzgeber klare Festlegungen zu treffen, was ein *schweres Verbrechen* ist.
2. Der Eingriff muss im Einzelfall gründlich geprüft und genehmigt werden. Es kann nicht sein, dass der Verfassungsschutz selbst entscheidet, welche Rechner er hacken darf, oder dass das BKA ohne juristische Kontrolle unliebsame Websites sperrt.

3. Ähnlich wie bei Hausdurchsuchungen ist eine Offenheit der Maßnahme anzustreben. Um Betroffenen die Gelegenheit zu geben, Rechtsmittel gegen ungerechtfertigte Bespitzelung einzulegen, ist eine Informationspflicht nach Abschluss der Maßnahme vorzusehen.

Das Bundesverfassungsgericht hat mehrfach die Einhaltung verfassungsrechtlicher Vorgaben angemahnt. Leider werden diese Grundsatzurteile immer wieder ignoriert. Ausschnitte aus einigen lesenswerten Begründungen:

- *”Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.”* (Bereits 1983 wies der 1. Senat des Bundesverfassungsgerichts in seiner [Urteilsbegründung zum Volkszählungsgesetz](#) darauf hin, dass durch die grenzenlose Nutzung moderner Datenverarbeitungsanlagen ein psychischer Druck auf den Einzelnen entsteht, sein Verhalten aufgrund der öffentlichen Anteilnahme anzupassen.)
- *”Inzwischen scheint man sich an den Gedanken gewöhnt zu haben, dass mit den mittlerweile entwickelten technischen Möglichkeiten auch deren grenzenloser Einsatz hinzunehmen ist. Wenn aber selbst die persönliche Intimsphäre ... kein Tabu mehr ist, vor dem das Sicherheitsbedürfnis Halt zu machen hat, stellt sich auch verfassungsrechtlich die Frage, ob das Menschenbild, das eine solche Vorgehensweise erzeugt, noch einer freiheitlich- rechtsstaatlichen Demokratie entspricht.”* (Aus dem Sondervotum der Richterinnen R. Jaeger und C. Hohmann- Dennherdt des 1. Senates des Bundesverfassungsgerichts zum Großen Lauschangriff 2004.)

9 Ich habe doch nichts zu verbergen

Dies Argument hören wir oft. Haben wir wirklich nichts zu verbergen? Einige Beispiele sollen exemplarisch zeigen, wie willkürlich gesammelte Daten unser Leben gravierend beeinflussen können:

- Im Rahmen der Zulässigkeitsprüfung für Piloten wurde Herr J. Schreiber mit folgenden vom Verfassungsschutz gesammelten Fakten konfrontiert: <http://www.pilotundflugzeug.de/artikel/2006-02-10/Spitzelstaat>
 1. Er wurde 1994 auf einer Demonstration kontrolliert. Er wurde nicht angezeigt, angeklagt oder einer Straftat verdächtigt, sondern nur als Teilnehmer registriert.
 2. Offensichtlich wurde daraufhin sein Bekanntenkreis durchleuchtet.
 3. Als Geschäftsführer einer GmbH für Softwareentwicklung habe er eine vorbestrafte Person beschäftigt. Er sollte erklären, welche Beziehung er zu dieser Person habe.
 4. Laut Einschätzung des Verfassungsschutzes neige er zu politischem Extremismus, da er einen Bauwagen besitzt. Bei dem sogenannten *Bauwagen* handelt es sich um einen Allrad-LKW, den Herr S. für Reisen nutzt (z.B. in die Sahara).

Für Herrn S. ging die Sache gut aus. In einer Stellungnahme konnte er die in der Akte gesammelten Punkte erklären. In der Regel wird uns die Gelegenheit einer Stellungnahme jedoch nicht eingeräumt.

- Ein junger Mann meldet sich freiwillig zur Bundeswehr. Mit sechs Jahren war er kurzzeitig in therapeutischer Behandlung, mit vierzehn hatte er etwas gekifft. Seine besorgte Mutter ging mit ihm zur Drogenberatung. In den folgenden Jahren gab es keine Drogenprobleme. Von der Bundeswehr erhält er eine Ablehnung, da er ja mit sechs Jahren eine Psychotherapie durchführen musste und Drogenprobleme gehabt hätte.
<http://blog.kairaven.de/archives/998-Datenstigmaanekdot.html>
- Kollateralschäden: Ein großer deutscher Provider liefert falsche Kommunikationsdaten ans BKA. Der zu Unrecht Beschuldigte erlebt das volle Programm: Hausdurchsuchung, Beschlagnahme der Rechner, Verhöre und sicher nicht sehr lustige Gespräche im Familienkreis. Die persönlichen und wirtschaftlichen Folgen sind nur schwer zu beziffern.
<http://www.lawblog.de/index.php/archives/2008/03/11/provider-liefert-falsche-daten-ans-bka/>

Noch krasser ist das Ergebnis der *Operation Ore* in Großbritannien. 39 Menschen, zu Unrecht wegen Konsums von Kinderpornografie verurteilt, haben Selbstmord begangen, da ihnen alles genommen wurde.
http://en.wikipedia.org/wiki/Operation_Ore

- “Leimspur des BKA”: Wie schnell man in das Visier der Fahnder des BKA geraten kann, zeigt ein Artikel bei Zeit-Online. Die Websites des BKA zur Gruppe “mg” ist ein Honeypot, der dazu dient, weitere Sympathiesanten zu identifizieren. Die Bundesanwaltschaft verteidigt die Maßnahme als legale Fahndungsmethode.

Mit dem im Juni 2009 beschlossenen BSI-Gesetz übernimmt die Behörde die Aufzeichnung und unbegrenzte Speicherung personenbezogener Nutzerinformationen wie IP-Adressen, die bei der Online-Kommunikation zwischen Bürgern und Verwaltungseinrichtungen des Bundes anfallenden. Wir können daraus nur den Schluss ziehen, diese und ähnliche Angebote in Zukunft ausschließlich mit Anonymisierungsdiensten zu nutzen.

Nicht immer treten die (repressiven) Folgen staatlicher Sammelwut für die Betroffenen so deutlich hervor. In der Regel werden Entscheidungen über uns getroffen, ohne uns zu benachrichtigen. Wir bezeichnen die (repressiven) Folgen dann als Schicksal.

Politische Aktivisten

Wer sich politisch engagiert und auf gerne vertuschte Mißstände hinweist, hat besonders unter der Sammelwut staatlicher Stellen zu leiden. Wir möchte jetzt nicht an Staaten wie Iran oder China mäkeln. Einige deutsche Beispiele:

1. Erich Schmidt-Eenboom veröffentlichte 1994 als Publizist und Friedensforscher ein Buch über den BND. In den folgenden Monaten wurden

er und seine Mitarbeiter vom BND ohne rechtliche Grundlage intensiv überwacht, um die Kontaktpersonen zu ermitteln. Ein Interview unter dem Titel *“Sie beschatteten mich sogar in der Sauna”* steht online: <http://www.spiegel.de/politik/deutschland/0,1518,384374,00.html>

2. Fahndung zur Abschreckung: In Vorbereitung des G8-Gipfels in Heiligendamm veranstaltete die Polizei am 9. Mai 2007 eine Großrazzia. Dabei wurden bei Globalisierungsgegnern Rechner, Server und Materialien beschlagnahmt. Die Infrastruktur zur Organisation der Proteste wurde nachhaltig geschädigt. Wenige Tage nach der Aktion wurde ein Peilsender des BKA am Auto eines Protestlers gefunden.
Um die präventiven Maßnahmen zu rechtfertigen wurden die Protestler als terroristische Vereinigung eingestuft. Das Netzwerk ATTAC konnte 1,5 Jahre später vor Gericht erreichen, dass diese Einstufung unrechtmäßig war. Das Ziel, die Organisation der Proteste zu behindern, wurde jedoch erreicht.
3. Dr. Rolf Gössner ist Rechtsanwalt, Vizepräsident der Internationalen Liga für Menschenrechte, Mitherausgeber des Grundrechte-Reports, Vizepräsident und Jury-Mitglied bei den Big Brother Awards. Er wurde vom Verfassungsschutz 38 Jahre lang überwacht. Obwohl das Verwaltungsgericht Köln bereits urteilte, dass der Verfassungsschutz für den gesamten Bespitzelungszeitraum Einblick in die Akten gewähren muss, wird dieses Urteil mit Hilfe der Regierung ignoriert. Es werden Sicherheitsinteressen vorgeschoben!

Mit dem Aufbau der “neuen Sicherheitsarchitektur” bedeutet eine Überwachung nicht nur, dass der direkt Betroffene überwacht wird. Es werden Bekannte und Freunde aus dem persönlichen Umfeld einbezogen. Sie werden in der Anti-TerrorDatei gespeichert, auch ihre Kommunikation kann überwacht werden, es ist sogar möglich, Wanzen in den Wohnungen der Freunde zu installieren.