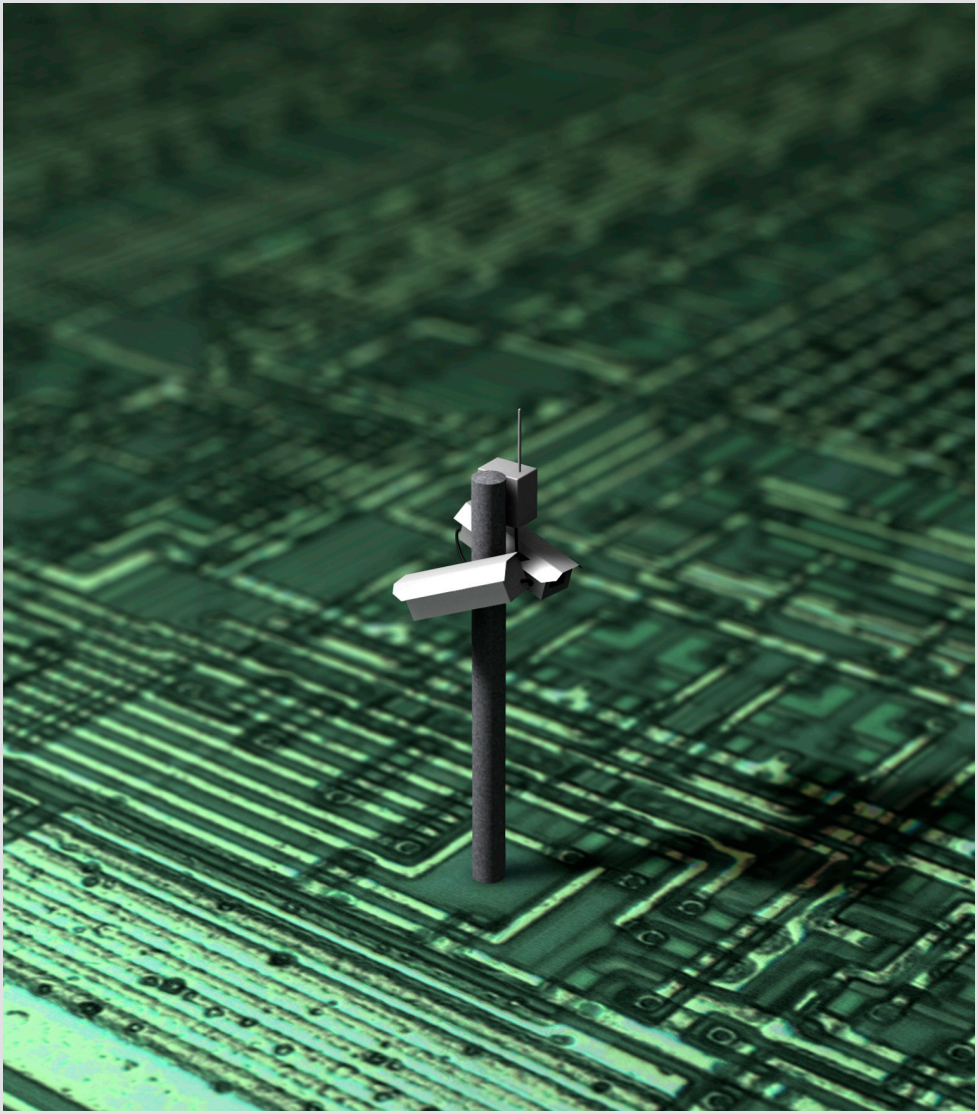
die datenschleuder.

das wissenschaftliche fachblatt für datenreisende
ein organ des chaos computer club



ISSN 0930-1054 • 2007
zwo punkt fünnef null euro stop
Kein Postvertriebsstück mehr ~~C11301F~~

#92


GRUND
GES
ÜBERWACHT
EUCH DOCH
SELBER

Die neue Ordnung heißt präventiver Sicherheitsstaat

Wir haben ja zusammen noch gefeiert bis Silvester. Die Ausnüchterung begann am 1. Januar 2008. Dann kam die Vorratsdatenspeicherung. Und was die jetzt nicht alles vorratsspeichern! Allein schon bei Telefonaten: Alle beteiligten Rufnummern und die Seriennummer der benutzten Geräte, die Dauer der Telefonate. Und bei Handys sogar den Standort, wann immer etwas ein- oder ausgeht. Ein schwacher Trost nur, daß wir uns dem neuerdings doch noch entziehen können. Und dazu müssen wir nicht einmal die Telefone wegwerfen. Es reicht schlicht, in die Nähe von Gefängnissen zu ziehen. Dort ist durch die Handy-Blocker ein bißchen Ruhe im GSM-Netz.

Und nach dem nächsten Congress? Kommt dasselbe in grün für das Internet: Die speichern unsere E-Mails. Inklusive aller Pharmapropaganda und Körperteilverlängerungen, dazu VoIP und Webseiten. Wir sind nicht einmal beim Pron-Surfen mehr alleine. Aber es sollte uns beruhigen zu wissen, daß es nicht der böse, an allen Ecken und Enden datenverlierende und für kein verkacktes IT-Großprojekt zu vorsichtige Staat ist, der dort die Informationen speichert. Nein! Wir können uns sicher sein, daß die zum Speichern gezwungenen Dienstleister alles in Hochsicherheitsinformationsendlagern versiegeln und einmotten werden. Allein schon, um sich vor dem Drang zu schützen, diese Daten selber zur Verbesserung der Kundenbeziehungen zu gebrauchen.

Aber was erdulden wir als gutgläubige Bürger nicht alles, wenn es gegen den bösen Terrorismus geht. Da können wir doch über kleine Kollateralschäden großzügig hinwegsehen. Aber halt! SPD-Innenspezialexperte Wiefelspütz klärt uns auf: „Ich wäre für die Vorratsdatenspeicherung auch dann, wenn es überhaupt keinen Terrorismus gäbe." Achso. Da trifft es sich ja gut, daß es hier tatsächlich keinen Terrorismus gibt, sondern wir in einem weitgehend friedlichen, nur selten von Terror-Tornados überflogenen Land leben, in dem sich selbst gewalttätige Sturmtruppen nur zu den üblichen Festspielen aus ihren Kasernen trauen. Und die sogenannten „Anschlagsversuche" fehlgeleiteter Jugendlicher wurden ganz ohne Bundestrojaner und Flugzeugabschuß verhindert. Doch ohne Feind war noch nie ein Staat zu machen.

Falls sich keiner mehr daran erinnert: Alle Fraktionen des Bundestages haben seinerzeit die Vorratsdatenspeicherung abgelehnt. Das hinderte Schily kein Stück, dem gefährlichen Mumpitz in Brüssel zuzustimmen und damit über den europäischen Umweg das Parlament zu mißachten. Und so soll es uns nicht wundern, daß dies nur eines in einer langen Liste von Gesetzen sein wird, das „materiell verfassungswidrig" ist. Der biometrische Paß, die Kennzeichen-Rasterfahndung, die „Anti-Terror-Datei" genannte Zentralkartei der nun verbundenen Repressionsbehörden, das geplante Bundeszentralregister mit lebenslanger Identifikation und nun die Computerwanze – die neue „Sicherheitsarchitektur" läßt sich doch nicht von so Kleinigkeiten wie dem Grundgesetz aufhalten. Es war ja auch nicht alles schlecht im Dritten Reich.

Wenn der Bürger nicht sowieso schon seit Jahren wüßte, daß Politiker korrupt, kriminalitätsanfällig und vollkommen merkbefreit sind, würde er zwischen Shoppen, Urlaub und unterbezahlter Arbeit vielleicht mal hochgucken, wenn Schäuble 2008 fordert, daß Hausdurchsuchungen wieder heimlich, Folter erlaubt und RFID-Implantate sowie akustische und visuelle Wohnraumüberwachung nun verpflichtend ist. Danach wählt er die Spacken beim nächsten Mal wieder – mangels sinnvoller Alternativen. Die Deutschen, die in Heerscharen jeden Monat das Land verlassen, sehen wohl keine Zukunft mehr hier. Es war ja auch nicht alles schlecht in der DDR.

Und um die zeitgenössischen Referenzen an totalitäre Systeme komplett zu machen, borgen sie auch noch bei Orwell: Die 129a-Verfahren bringen uns nun endlich auch in Deutschland Gedankenverbrechen, deren Reichweite mit der Wiedereinführung der möglichst unscharfen „Vorfelddelikte" weiter ausgebaut wird. Mit der Online-Durchsuchung hätten sich ja gewiß

Bundesinnenminister Schäuble läßt sich extra für den Photographen von dem Kollegen, der ihm üblicherweise das Internet ausdruckt, selbiges „erklären". Man achte auch auf die Prachtausgabe des Koran im Hintergrund, das Deutsch-Arabisch-Wörterbuch und den Hardware-Prototypen des Bundestrojaners direkt links neben dem Bildschirm, bei Conrad als KVM-Switch im Angebot.

noch mehr verbotene Gedanken finden lassen. Die Sicherheitshysteriker an der Spitze des Bundesinnenministeriums werden ja nicht müde, weiter ohne Unterlaß ihren Trojaner zu fordern.

Wenn man genauer hinsieht, entdeckt man aber auch zutiefst menschliche Seiten im Überwachungsapparat: Zum ersten gibt es praktisch keine Vertreter des Innen- oder Justizministeriums mehr, die diese beispiellose Ermächtigung der „Sicherheits"behörden öffentlich mit so etwas Ähnlichem wie inhaltlichen Argumenten verteidigen. Wir glauben ja inzwischen: verteidigen könnten. Die zweite Beobachtung ist noch beunruhigender: Nahezu jeder Beamte, der das Räderwerk des Neuen Deutschen Überwachungsstaates bedient, sagt im Privaten, daß er das eigentlich auch total überzogen und in seiner Gesamtheit sehr erschreckend findet. Aber – leider, leider – man kann ja nix machen. Befehle sind Befehle, und wo kämen wir denn hin, wenn in Deutschland plötzlich keine Befehle mehr befolgt würden.

Immerhin scheinen die IT-Angestellten der Polizei in Scharen die Flucht in die Wirtschaft anzutreten. Wer will auch schon für ein Scheißgehalt einen moralisch äußerst fragwürdigen Job machen, wenn es Alternativen gibt. Dieser Trend ist förderungswürdig. Und nur für den Fall, daß ihr jemanden kennt, der nach dem Ausstieg aus der Informationsjunkieszene sein Gewissen erleichtern und Details mit anderen interessierten Nerds teilen möchte, ist der Braune-Umschläge-Schlitz an der Redaktion Datenschleuder rund um die Uhr geöffnet.

Nein, eine Grenze hat Tyrannenmacht.
Wenn der Gedrückte nirgends Recht kann finden,
wenn unerträglich wird die Last - greift er
hinauf getrosten Mutes in den Himmel
Und holt herunter seine ew'gen Rechte,
die droben hangen unveräußerlich
und unzerbrechlich wie die Sterne selbst.

Friedrich Schiller, Wilhelm Tell

Und als Paukenschlag der Weitsicht trifft uns just beim Schreiben dieser Zeilen das Geschenk des Bundesverfassungsgerichts. Es waren Backpfeifen in die terrorgeifernden Fressen der berufsmäßigen Gesetzesverkacker, jede einzelne Schelle so präzise plaziert, wie es in letzter Zeit leider nur noch die obersten Richter dieser Republik vermögen.

Sie sind die letzte Bastion der Vernunft vor den immer wieder Grenzen auslotenden Heerscharen digitaler Analphabeten in den ministerialen Chefsesseln. Denn daß deren Ignoranz **doch** keine Frage der Generation ist, beweisen die roten Roben so beiläufig, wie sie beim verfassungsrechtlichen Betonieren der digitalen Selbstverständlichkeiten mit Dampfhammerschlägen links und rechts des Weges gleich noch die Vorratsdatenspeicherung und die Praxis der Rechnerbeschlagnahme auf Punktmasse zusammenstampfen.

Zu unserem neuen Wau-Holland-Gedenk-Grundrecht möchte die Redaktion allen Lesern herzlich gratulieren. Zwar hat das neue Recht den für Nichtjuristen etwas sperrig auszusprechenden Namen „Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit von informationstechnischen Systemen“, aber wir haben uns schließlich auch daran gewöhnt, den Zungenbrecher „informationelle Selbstbestimmung“ fehlerfrei auszusprechen.

Wir können nun, kaum 25 Jahre nach Proklamation der Netzweltlobby, stolz darauf sein, mit unserer Agenda den gesellschaftlichen Mainstream durchdrungen zu haben. Uns wurde eine absolut geschützte digitale Intimsphäre geschenkt und die Bedeutung der Verschlüsselung dabei besonders betont.

Und wir wünschen uns und euch, daß dieses neue Grundrecht wahrgenommen und im Grossen wie im Kleinen mit Zähnen und Klauen verteidigt wird. Aber auch, daß wir dieses Grundrecht aller unserer Mitmenschen respektieren.

<die redaktion>

Inhalt

Erfa-Kreise / Chaostreffs

Bielefeld, CCC Bielefeld e.V., Bürgerwache Siegfriedplatz
freitags ab 20 Uhr *http://bielefeld.ccc.de/ :: info@bielefeld.ccc.de*

Berlin, CCCB e.V. (Club Discordia) Marienstr. 11, (✉ CCCB, Postfach 64 02 36, 10048 Berlin)
donnerstags ab 17 Uhr *http://berlin.ccc.de/ :: mail@berlin.ccc.de*

Darmstadt, chaos darmstadt e.V. TUD, S2|02 E215
dienstags ab 20 Uhr *https://www.chaos-darmstadt.de :: info@chaos-darmstadt.de*

Dresden, C3D2/Netzbiotop e.V., Lingnerallee 3, 01069 Dresden
dienstags ab 19 Uhr *http://www.c3d2.de :: mail@c3d2.de*

Düsseldorf, CCCD/Chaosdorf e.V., Fürstenwall 232, 40215 Düsseldorf
dienstags ab 19 Uhr *http://duesseldorf.ccc.de/ :: mail@duesseldorf.ccc.de*

Erlangen/Nürnberg/Fürth, BitsnBugs e.V. "E-Werk", Fuchsenwiese 1, Gruppenraum 5
dienstags ab 19 Uhr *http://erlangen.ccc.de/ :: mail@erlangen.ccc.de*

Hamburg, Lokstedter Weg 72
2. bis 5. Dienstag im Monat ab etwa 20 Uhr *http://hamburg.ccc.de/ :: mail@hamburg.ccc.de*

Hannover, Leitstelle 511 e.V., c/o Bürgerschule Nordstadt, Schaufelder Str. 30, 30167 Hannover
jeden 2. Mittwoch und jeden letzten Dienstag im Monat ab 20 Uhr *https://hannover.ccc.de/*

Karlsruhe, Entropia e.V. Gewerbehof, Steinstr. 23
sonntags ab 19:30 Uhr *http://www.entropia.de/ :: info@entropia.de*

Kassel, Uni Kassel, Wilhelmshöher Allee 71-73 (Ing.-Schule)
1. Mittwoch im Monat ab 18 Uhr *http://kassel.ccc.de/*

Köln, Chaos Computer Club Cologne (C4) e.V., Vogelsanger Straße 286, 50825 Köln
letzter Donnerstag im Monat ab 20 Uhr *https://koeln.ccc.de :: mail@koeln.ccc.de*

München, muCCC e.V. jeden 2. Dienstag im Monat ab 19:30 Uhr *http://www.muc.ccc.de/*
jeden Dienstag Treffen des Infrastrukturprojekts *https://kapsel.muc.ccc.de/*

Ulm, Café Einstein an der Uni Ulm, montags ab 19:30 Uhr *http://ulm.ccc.de/ :: mail@ulm.ccc.de*

Wien, chaosnahe gruppe wien Kaeuzchen, 1070 Wien, Gardegasse (Ecke Neustiftgasse)
alle zwei Wochen, Termine auf Webseite *http://www.cngw.org/*

Zürich, CCCZH, c/o DOCK18, Grubenstrasse 18 (✉ Chaos Computer Club Zürich, Postfach, CH-8045 Zürich),
abwechslungsweise Di/Mi ab 19 Uhr *http://www.ccczh.ch/*

Aus Platzgründen können wir die Details aller Chaostreffs hier nicht abdrucken. Es gibt aber in den folgenden Städten Chaostreffs mit Detailinformationen unter *http://www.ccc.de/regional/*: Aachen, Aargau, Augsburg, Basel, Bochum, Bristol, Brugg, Dortmund, Frankfurt am Main, Freiburg im Breisgau, Gießen/Marburg, Hanau, Heidelberg, Ilmenau, Kiel, Leipzig, Mainz, Mülheim an der Ruhr, Münster/Osnabrück, Offenbach am Main, Paderborn, Regensburg, Rheintal in Dornbirn, Stuttgart, Trier, Weimar, Wetzlar, Wuppertal, Würzburg.

Zur Chaosfamilie zählen wir (und sie sich) die Häcksen (*http://www.haecksen.org/*), den FoeBuD e.V. (*http://www.foebud.org/*), den Netzladen e.V. in Bonn (*http://www.netzladen.org/*) und die c-base Berlin (*http://www.c-base.org/*).

Die Datenschleuder Nr. 92

Herausgeber (Abos, Adressen, Verwaltungstechnisches etc.)

Chaos Computer Club e.V., Lokstedter Weg 72,
20251 Hamburg, Fon: *+49.40.401801-0,*
Fax: *+49.40.401801-41, <office@ccc.de>* Fingerprint*:*
1211 3D03 873F 9245 8A71 98B9 FE78 B31D E515 E06F

Redaktion (Artikel, Leserbriefe, Inhaltliches etc.)

Redaktion Datenschleuder, Pf 64 02 36, 10048 Berlin,
Fon: +49.30.28097470, *<ds@ccc.de>* Fingerprint:
03C9 70E9 AE5C 8BA7 42DD C66F 1B1E 296C CA45 BA04

Druck Pinguindruck Berlin, *http://pinguindruck.de/*

ViSdP Dirk Engling *<erdgeist@erdgeist.org>*.

Chefredaktion

46halbe, starbug und erdgeist.

Layout

evelyn, rpk, 46halbe, starbug und erdgeist.

Redaktion dieser Ausgabe

46halbe, starbug, Lars Sobiraj, Marco Gercke, Julian Finn, Martin Haase, Henryk, Frédéric Phillip Thiele, Henrik Speck, LeV, Sandro Gaycken, saite, erdgeist.

Die Welt von morgen: Mitro AG: 15 Jahre mit Sicherheit Erfolg

Leserbriefe gesammelt von Martin Haase

Vor 15 Jahren, am 23. Mai 2018 schlossen sich die wichtigsten Dienstleister im Bereich Handel, Banken, Versicherungen, Security und Kommunikation zur Mitro AG zusammen. Seitdem haben Freiheit und Sicherheit einen neuen Namen: Mitro.

Zahlreiche unserer innovativen Produkte fanden ihren Weg auf den Markt, den wir inzwischen beherrschen. Vor allem das vor fünf Jahren eingeführte Rundum-Sorglos-Paket *miLife* erfreut sich großer Beliebtheit, denn es regelt alle Probleme des Alltags. Die Verbindung von Überwachung, Versicherung, Dienstleistung und Handel erschließt ganz neue Möglichkeiten für eine sichere finanzielle Entwicklung unseres Konzerns, von dem viele Aktionäre und Kunden profitieren. Wir veröffentlichen hier eine Auswahl aus den Zuschriften unserer begeisterten Kunden:

Frau K. aus S. schrieb:

Liebe Mitro-AG,

seit ich Kundin bei Mitro bin, hat sich mein Leben grundlegend verändert. Dank *miLife* kümmert sich Mitro um alles. Ich brauche nicht einmal mehr daran zu denken, meinen Kühlschrank aufzufüllen, denn ich werde immer mit den Produkten beliefert, die ich wirklich benötige und die ich mag. Dabei wird auch noch darauf geachtet, daß ich mich richtig ernähre, denn *miLife* beinhaltet ja auch die ärztliche Versorgung bei den hervorragenden Mitro-Ärzten. Auch Mitro-TV, das mich mit meinen Lieblingsprogrammen auf meinem *miPod Mega* versorgt, gefällt mir richtig gut! Sie treffen genau meinen Geschmack! Meine Lieblingssendung ist *miBigBrother*, in der Sie immer wieder sehr interessante Einblicke in die Privatsphäre der von Ihnen überwachten Kunden zeigen. Ich selbst gehöre auch zu den 12 Millionen *miCam*-Nutzern, die sich freiwillig hierfür gemeldet haben. Leider haben Sie noch nie Bilder aus meiner Wohnung gezeigt! Besonders bedanken möchte ich mich für meinen letzten Urlaub, den Mitro für mich organisiert hat. Im ihrem Mitro-Hotel habe ich mich sehr gut erholt! Die neuen *miCams* in meiner Wohnung, einem *miHome*, passen wunderbar zur Einrichtung. Alle meine Besucher sind begeistert und wollen sich auch von den *miCams* filmen lassen. Wie kann ich die Überwachungsaufnahmen meiner Gäste abrufen, um ihnen eine Auswahl zu überlassen?

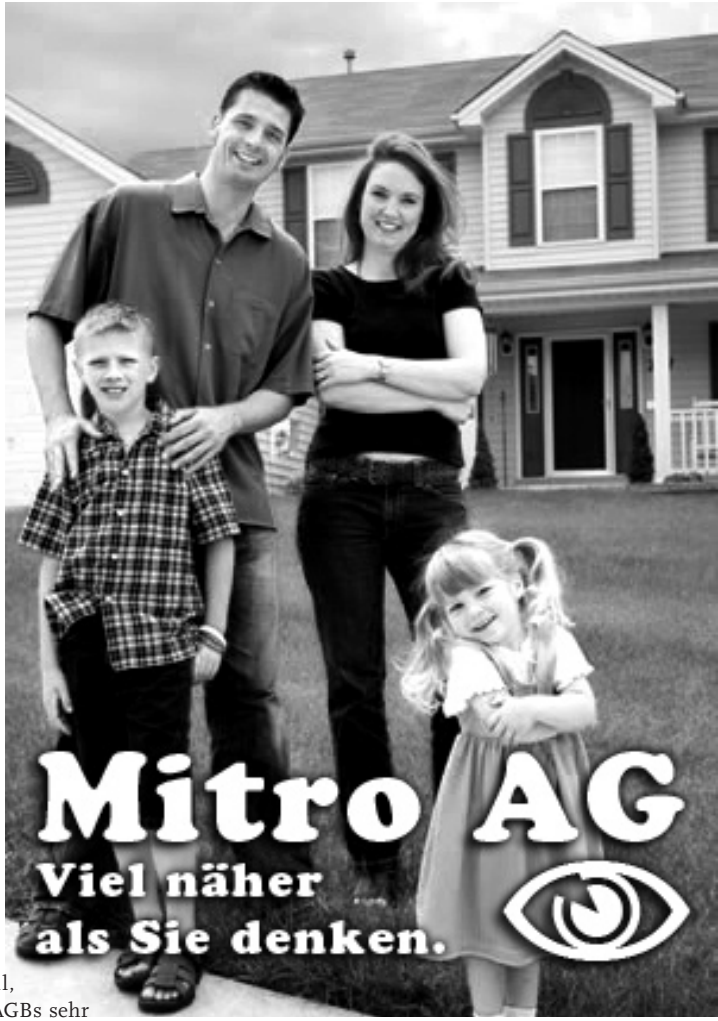
Die Rentnerin S. aus Q. schrieb:

Seit meine Wohnung komplett von Mitro überwacht wird, fühle ich mich endlich sicher. Für uns Ältere geht es ja nicht nur um den Schutz vor Dieben und Trickbetrügern an der Haustür, sondern auch darum, daß in unserer Wohnung jemand über uns wacht. Ich hatte immer entsetzliche Angst, daß ich einmal hinfalle und mir selbst nicht helfen kann. Damit ist dank *miSenior* nun Schluß! Wenn mir etwas passiert, ist sofort ein Mitro-Arzt da und kann mir helfen. Auch als meine Katze neulich verschwunden war, konnte sie dank des RFID-Chips sofort wiedergefunden werden.

Die Staatsrechtlerin Claudia R. aus U.

äußerte sich in ihrem unabhängigen Gutachten positiv über die Auswirkungen unserer Angebote auf Staat und Gesellschaft:

Besonders dank der umfassenden Lebensgestaltungs- und (Ver-)Sicherungsangebote von großen Anbietern wie Mitro konnte das Rechtssystem deutlich entschlackt werden. Komplizierte Regelungen des Zivil- und Strafrechts konnten entfallen, weil die Allgemeinen Geschäftsbedingungen dieser Dienstleister eine positive Auswirkung auf die Gesellschaft haben; nehmen wir als Beispiel das erfolgreichste Produkt seiner Art: *miLife* von Mitro:



- Dieses Produkt regelt alle Bereiche des Lebens und schließt eine komplette Be- und Überwachung der Kunden in deren eigenem Interesse ein. Damit wird der Staatsschutz stark entlastet, zumal die Ermittlungsbehörden im Bedarfsfall direkten Zugriff auf alle Daten haben, sofern die Ermittlungen nicht ohnehin von Mitro selbst durchgeführt werden.

- Da niemand aus dem *miLife*-Dienstleistungssystem ausscheiden will, beachten die Kunden die AGBs sehr genau, was sich ebenfalls positiv auf die Gesellschaft auswirkt.

- Der Wunsch nach einer flächendeckenden Überwachung ist bei *miLife*-Kunden so groß, daß sich die Zahl der Kameras besonders in den Wohngegenden vervielfältigt hat – mit einem positiven Effekt für die öffentliche Sicherheit. Da es sich um private Überwachungsanlagen handelt, entstehen der öffentlichen Hand keine Kosten.

Dank des privaten Engagements für Überwachung, Recht und Ordnung erleben wir die Befreiung des Bürgers aus der Bevormundung des Staats. Jeder kann sich sein Lebens-Produkt frei auswählen. Die noch vor einigen Jahren oft beschworene Gefahr eines Überwachungsstaats ist gebannt, denn nun kümmern sich private Firmen um Sicherheit, und jeder Bürger kann sich selbst sein Sicherheitspaket schnüren.

Die Ergänzungsprogramme *miKid* und *miEdu* entlasten die Bildungsbudgets, denn das öffentliche Schul- und Hochschulsystem wurde praktisch überflüssig und größtenteils durch private Einrichtungen ersetzt. Auch die öffentlichen Ausgaben für Kunst und Kultur konnten dank Mitros Einsatz in diesen Bereichen reduziert werden.

Zwar verursacht die höhere Lebenserwartung von *miLife*-Kunden Mehrausgaben in der Krankenversorgung, die jedoch dadurch ausgeglichen werden, daß *miLife* auch die komplette Krankenversorgung im Mitro-eigenen Gesundheitssystem umfaßt und somit ein staatliches Solidarsystem überflüssig wird. Viele Mitro-Kliniken sind auch Einrichtungen der medizinischen und pharmazeutischen Forschung und ermöglichen es Mitro daher, neueste Forschungserkenntnisse gleich an die Patienten weiterzugeben und damit auch wieder die Forschung voranzubringen.

(Prof. Claudia R. lehrt an der Mitro-Hochschule für Recht und Ordnung.)

Herr S. aus M. schrieb:

Ich möchte Ihnen besonders danken, daß Sie mich trotz meiner mir sehr unangenehmen Verstöße gegen Ihre AGBs nicht aus ihrem *miLife*-Programm ausgeschlossen haben, wie es meiner Schwester geschehen war, die bei Ihrer Konkurrenz ein vergleichbares Produkt hatte. Als sie niemand mehr in ein Versicherungs- und Versorgungsprogramm aufnehmen wollte, halfen Sie ihr mit Ihrem Resozialisierungsprogramm *Any Other Life* über das Schlimmste hinweg, und sie konnte als Leihmutter und Organspenderin wieder zu einer zahlenden Konsumentin werden. Leider ist sie im letzten Jahr verstorben – zu früh, denn sie konnte die hervorragende *miLife*-Gesundheitsversorgung nicht in Anspruch nehmen. Auch in ihrem Namen möchte ich Ihnen danken.

Olaf M. (7) aus T. schrieb:

Meine Ältern Haben mir ein *miKid*-paket geschänkt. Die Vielen Spiele und die Kamara sind SCHÖN! Auch das Fahrrad dass mir Lena jetzt nicht mehr klauen kann, wegen dem Schipp.

Laubenkolonie Argus aus B. schrieb:

Das Konzept der Community-Überwachung der Mitro AG hat uns sofort überzeugt. Von jeder Gartenlaube aus kann unsere ganze Kolonie überwacht werden. Die Kameras gliedern sich sehr schön in die Anlage ein. Da viele von uns schon *miLife*-Nutzer sind, fiel uns die Bedienung der Kameras sehr leicht. Nun wird bei uns niemand mehr ungestraft über die Blumenbeete gehen oder am Sonntag seinen Rasen mähen. Das Gemeinschaftsgefühl hat sich sehr verbessert!

Frau von R. aus K. schrieb:

Nach dem verfrühten Tod meines verehrten Gatten, der sich von den Vorteilen des *miLife*-Pakets zu Lebzeiten leider nicht überzeugen lassen wollte, habe ich meine Vermögensverwaltung vollständig an Mitro übergeben. Seither wächst mein Vermögen stetig, und ich kann mich ganz dem Golfspiel widmen – selbstverständlich auf den Mitro-Golfplätzen, die zu den schönsten und sichersten der Welt gehören.

Psalm 23

Der Herr ist uns Hirte und uns wird nichts mangeln,
nicht Freiheit, nicht Würde, wenn er uns behütet.
Er führt uns auf sicheren Pfaden und Angern
und wacht über alle und alles mit Güte.

Wo immer wir wandeln, da schaut uns sein Auge,
beim Shoppen, beim Bummeln und beim Demonstrieren,
beobachtet, speichert. Er weiß, was wir taugen.
Er sieht, wenn wir heimlich auf Klo masturbieren.

Er waltet und prüft, ob wir wider ihn sprechen,
Gebote befolgen, Gesetztes zerbrechen.
Wir sind seine Sklaven, denn wir fürchten die Strafe.
Wir preisen dich Hirte, du hütest uns Schafe.

LeV

Warum eigentlich nicht?

Sandro Gaycken <sandro@berlin.ccc.de>

Das Thema Datenschutz krankt leider immer wieder an einer ganz bestimmten Front: dem Problem Problembewußtsein. Warum eigentlich Datenschutz? Geht es wirklich nur um das persönliche Empfinden – wo, wieviel und welche Privatheit man für sich gerne hätte? Und dies im Verhältnis zur Sicherheit vor Terroristen und nützlichen Verbraucherinformationen?

Nein! Natürlich nicht. Aber die harten, faktischen Argumente, worum es eigentlich geht, stehen leider noch viel zu oft viel zu weit hinter den rein technischen Beschreibungen. Wenn das Bedürfnis nach Sicherheit das Bedürfnis nach Privatsphäre in einem Maße übersteigt, das die entsprechenden Überwachungsmaßnahmen legitimiert, warum soll man dann nicht einen neuen sozialen Deal in der Gesellschaft dazu aushandeln? Wenn man nur die als irrelevant empfundenen Teile seiner Privatsphäre anonymen Programmen überläßt. Wenn diese daraus Profile erstellen, die ausschließlich vor terroristischen Gefahren schützen und über nützliche Produkte und Angebote informieren, was ist dann bitte daran so schlecht? Warum eigentlich nicht?

Totschlagargumente

Diese ganze Art des Argumentierens kennen wir. Und Aktivisten wie wir haben das leidige Problem, dagegen anzuargumentieren. Und meist läuft das darauf hinaus, daß man selbst schlicht anders empfindet und größeren Wert auf Privatsphäre legt als andere. Aber das subjektive Wertempfinden allein, das in der medial urteilenden Gesellschaft zudem gerade eher gegen Terror als gegen Überwachung gestimmt ist – und man kann nur eins von beiden haben –, bietet keine solide Grundlage für Gegenargumente. Der eine fühlt sich so, der andere eben so.

Aber was dann? Sind wir vielleicht wirklich nur Alarmisten am Rande? Natürlich nicht. Denn Datenschutz ist Schutz von Freiheit, und Freiheit ist ein wichtiges Gut. Das ist ja auch unser Credo, unsere Intuition, die wir verteidigen: Gibst Du Deinen Datenschutz auf, dann gibst Du große Teile Deiner Freiheit auf. Und gibst Du erstmal Deine Freiheit auf, dann hast Du bald gar nichts mehr. Das ist ja auch richtig. Und wenn man aus der Geschichte noch etwas anderes lernen könnte als daß man nichts aus der Geschichte lernt: Das wäre sicher das Naheliegendste.

Leider bieten diese Intuitionen allein keine solide Basis für Verständnis mehr, denn andere empfinden durch den Dunst des Sicherheitswahns mit abnehmender Klarheit. Was man also als Datenschützer unbedingt auch argumentativ zeigen muß, sind gerade exakt die genauen Verbindungen von Datenschutz und Freiheit. Die starken, faktischen Argumente müssen dabei gebracht werden. Daher will ich an dieser Stelle noch einmal drei solcher Argumente liefern, mit einigen kleineren Teilargumenten. Einige dieser Argumente wurden bereits diskutiert, andere sind neu.

Profiling

Das erste Argument bezieht sich auf Profiling durch Data-Miner. Diese produzieren im Profiling stereotype Profile von Menschen aufgrund einiger Rahmendaten ihres Verhaltens. Das Problem dabei ist nun erst einmal, daß stereotype Profile nicht mit der echten Person übereinstimmen müssen. Das wird auch nicht nachgeprüft. Trotzdem aber werden die Profile als Grundlagen für wichtige Urteile benutzt. So werden etwa Annahmen über Kreditfähigkeit angestellt, über kulturelle und sexuelle Präferenzen, über Gesundheit, zu erwartende Lebensdauer und Risikobereitschaft, und alle diese Annahmen werden von Versicherungen, von Banken und vielen anderen Unternehmen und dem Staat genutzt, um Personen zu bewerten.

Dabei kann es vielfach zu ungerechtfertigten Urteilen kommen – von der Ablehnung eines Kredits oder einer Versicherung bis zur langjährigen Inhaftierung in den USA. Denn die Daten sind ja nicht überprüft, und so urteilt man über Menschen ohne eine genaue Beweislage, sozusagen nur nach äußerst vagen Indizien. Das ist eine schlechte Sache daran. Was aber noch schlimmer ist, ist der Umstand, daß inzwischen ganze Gesellschaften nach Profilgruppen geordnet werden. Das ist gleichbedeutend mit einer neuen sozialen Klassenbildung: Eine Data-Miner-Klassengesellschaft entsteht.

Überwachung in Form des Data-Mining produziert also soziale Ungerechtigkeit, indem sie die Menschen ohne Einflußmöglichkeiten aufgrund spekulativer Annahmen in eine Profil-Klassengesellschaft ordnet, die trotz ihrer Spekulativität als Entscheidungsgrundlage für viele lebensrelevante Bereiche genutzt wird.

Verhaltensänderungen

Das zweite Argument besteht aus mehreren kleineren Argumenten. Erstens kann man betonen, daß in einer Gesellschaft, in der die gesellschaftliche Konformität des Verhaltens streng überwacht wird, die Fähigkeit zum eigenständigen ethischen Handeln verkümmert. Das ergibt sich zum einen faktisch. Denn wenn die meisten Werthandlungen gesellschaftlich vorausgenommen sind und in einer dauerüberwachten Konformität alternatives Denken nicht herangezogen werden muß, wird dieses Denken auch nicht mehr kulturell gepflegt.

Diese psychologische Phänomen kann man auch bei überbemutterten Kindern beobachten. Die sind es nämlich gewohnt, daß jemand anderes für sie Werturteile trifft und daher selbst nicht ohne weiteres dazu in der Lage. Eine dauerüberwachte Gesellschaft macht also Ethik überflüssig und führt zur Verkümmerung der entsprechenden Entscheidungskapazitäten.

Zweitens kann man auch Schwierigkeiten für die Identitätsbildung von Personen festhalten. Auch hier steht wieder ein psychologisches Phänomen im Hintergrund. Es entwickelt sich bei Dauerüberwachung und bei sozialer Vorsor-

tierung durch Profiling nämlich der Eindruck, daß man sich nicht mehr frei bewegen kann, daß man konform sein und auf Grenzüberschreitungen achten muß. Und dieser Eindruck generalisiert sich weiter als allgemeiner, gefühlter Konformitätszwang auf alle Lebensbereiche. Das klingt nach der von den Amerikanern des Kalten Krieges den Sowjets propagandistisch angedichteten Gleichschaltung. Dauerüberwachung und Profiling können also auch zu einer starken Einschränkung der Identitätsbildung führen.

Drittens läßt sich aus dieser Beobachtung noch eine weitere Bemerkung ableiten. Denn wenn durch Dauerüberwachung und Profiling keine Freiräume mehr für nonkonformes Verhalten vorhanden sind – weder faktisch noch im Geiste –, werden sich die sozialen Normen auch nicht ändern können, die den Rahmen dessen bilden, was aktuell als Konformität angesehen wird. Denn das Denken oder Austesten von Alternativen wird nahezu unmöglich.

Das ist vor allem schlecht, da nicht anzunehmen ist, daß die jetzigen Normen der Gesellschaft ewige Normen einer unter allen Bedingungen perfekten Gesellschaft sind. Ganz im Gegenteil: Man wird sinnvollerweise von ihnen erwarten müssen, daß sie Flexibilität mitbringen und sich den Wandlungen gesellschaftlicher Bedürfnisse und Notwendigkeiten entsprechend verändern lassen.

Ein Beispiel dafür ist die Schwulenbewegung. Hätte sie keinerlei Raum gehabt, eine Subkultur abseits der Normen zu unterhalten, wäre die inzwischen vollständig und breit gesellschaftlich akzeptierte Bewegung mit all ihren Rechten wahrscheinlich nie entstanden. Eine Überwachungsgesellschaft produziert also mit der faktischen und geistigen Abschaffung der Spielräume für Nonkonformität eine starre Gesellschaft, die nicht nur keine Änderungen zum Schlechten, sondern auch keine zum Guten mehr zulassen kann.

Solange wir allerdings noch keine perfekte Gesellschaft haben, kann das nicht wünschenswert sein. Und da wir auch nie eine perfekte Gesellschaft haben können, da dies auch immer von variablen Umwelt- und letztlich anderen Wertmaßstäben abhängt, wird das auch nie wünschenswert sein.

Grenzen und Normen

Das dritte Argument beschäftigt sich mit dem Unterschied von Überwachungsinfrastruktur und der gesellschaftlichen Regelung ihrer Nutzung.

Zuerst ist dafür festzuhalten, daß der gegenwärtige, möglicherweise subjektiv akzeptable Stand der Kosten-Nutzen-Abwägung ("ein bißchen Privatheit für mehr Sicherheit") lediglich ein aktueller Status Quo auf einer Skala ist, deren technisch mögliches Ende anders aussieht. Denn die technischen Mittel machen bei dem als noch irrelevant empfundenen Teil von Privatheit nicht prinzipiell halt.

Technisch möglich ist viel mehr, nämlich die lückenlose, allgegenwärtige Überwachung eines in Handeln und Denken nahezu vollständig transparenten Menschen. Diese Möglichkeit ergibt sich ganz nüchtern aus der Projektion der gegenwärtig in Entwicklung befindlichen Sicherheitssysteme. Technisch möglich ist also mit der sich gegenwärtig ausbauenden Infrastruktur der Überwachung noch sehr viel mehr. Das einzige, was nun die entsprechend interes-

sierten Nutzer davon abhält, sind die gegenwärtig ausgehandelten Regelungen der Nutzung.

Hier allerdings muß man jetzt sehen, daß diese nicht für alle Zeiten oder auch nur alle möglichen Nutzer bindend sind. Allein schon die gegenwärtigen Nutzungsregelungen beweisen da eine Dehnbarkeit, die sich schon in der vagen Definition des Begriffs "Terrorist" wiederfindet. Nicht einen Tag nach dem 11. September hat jeder zweite Staat seinen Intimfeind als Terroristen bezeichnet. Für Japan etwa sind Greenpeace-Aktivisten Terroristen, für die USA fast jeder Moslem, der einmal Flugunterricht genommen hat. Und Terroristen dürfen lückenlos überwacht und ge-profiled werden.

Es wird also eine Überwachungsinfrastruktur gebaut, die das Handeln und Denken ihrer potentiellen Feinde rein technisch gesehen immer allgegenwärtiger und immer lückenloser überwachen kann und deren Anwendungsfokus allein von der Definition vom "potentiellen Feind" abhängt. Das ist gerade der Unterschied zwischen Überwachungsinfrastruktur und der gesellschaftlichen Regelung der Nutzung. Die Infrastruktur macht vor der gegenwärtigen Nutzung nicht halt. Um zu sehen, wohin das dann geht, muß man sich nur überlegen, wer demnächst wen als potentiellen Feind definiert.

Auf den noch dezenten nächsten Schritten der Skala kann man dann die Versicherungen verorten, die jeden Versicherten als potentiellen Versicherungsbetrüger, jeden Raucher, Esser und Autofahrer als finanzielles Risiko einstufen und die sicher Interesse an den Daten über das Eß-, Fahr- und Freizeitverhalten haben, um jeden seiner Gewohnheiten gemäß einstufen und entsprechend ablehnen zu können.

Das Finanzamt sieht sich ja ohnehin nur von Steuerbetrügern umgeben, sodaß bestimmt auch dort bald Informationen über das Informations- und Konsumverhalten der Bürger gesammelt und ausgewertet werden dürften. Diese Optionen würden wohl auch den Durchschnittsbürger alarmieren und letztendlich nicht ganz gefallen. Rein technisch steht dem – wie gesagt – mit der gegenwärtigen Infrastruktur nichts mehr im Wege.

Noch viel schlimmer allerdings ist das extreme Ende der Skala, an dem wir einen totalitären Staat finden, der sich vollständig von seinen Bürgern abgekapselt hat und jeden als potentiellen Feind einstuft.

Gegen eine derart fiktive Extremisierung kann man natürlich sofort einwenden, daß man ja doch zwischen totalitären Überwachungsdys-

topien und der demokratisch-grundrechtlich geregelten Gegenwart unterscheiden muß. Allerdings gibt es – wie gesagt – eben keinen technisch-infrastrukturellen Unterschied mehr zwischen diesen beiden Extremen. In anderen Worten: Die technische Infrastruktur, die heute demokratisch-grundrechtlich geregelt entworfen und faktisch gebaut wird, ist die gleiche, die morgen totalitär-dystopisch genutzt werden kann und die in diesem Fall einem Diktator instantan eine unverschämte und nie dagewesene Macht und Stabilität verleihen würde.

Korrekt ausgerichtete Überwachungskamera

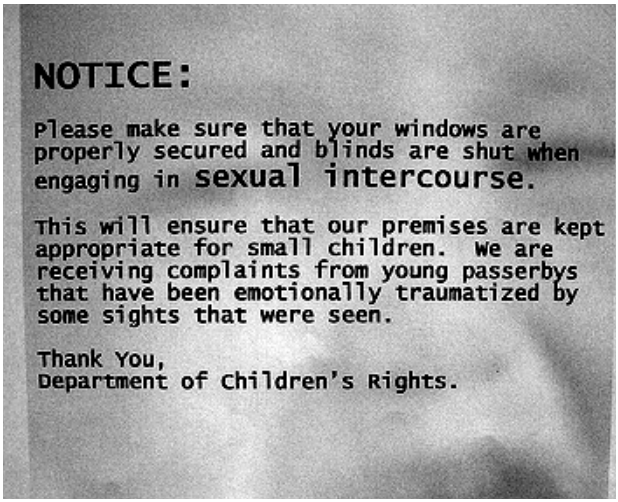
Jeder Andersdenkende, aller Widerstand, jeder definierte Feind wäre innerhalb von Sekunden aus Profildaten zusammenvermutet, mit seinem „Handy" lokalisiert und kann ohne Hoffnung auf Flucht verhaftet werden. Man stelle sich nur einmal vor, was wohl Hitler gemacht hätte, wenn er über das Internetverhalten jedes Einzelnen Bescheid gewußt hätte – wofür der sich wohl so interessiert. Wenn er von jeder Bezahlung jedes Bürgers gewußt hätte – was der so kauft und in seiner Freizeit macht. Wenn er wirklich jede Kommunikation zwischen Menschen maschinell hätte abhören können und jeden Menschen sofort lokalisieren.

In einer solchen Diktatur ist jede Hoffnung vergebens und die schlechte Nachricht dazu ist eben: Die Infrastruktur dafür hätten wir schon mal. Man baut also heute schon an der Stabilität der nächsten Diktatur, und es gibt an dieser Überwachungsinfrastruktur keinen Schalter, keine Sicherung, die den "gesellschaftlichen Mißbrauch" durch Diktatoren verhindern könnte. Wenn also eine unter ohnehin bereits fragwürdigen und unklaren Kompromissen und Kosten-Nutzen-Abwägungen erkaufte technische Infrastruktur vor Mißbrauch und Versagen mit extremen gesellschaftlichen Konsequenzen nicht geschützt werden kann, wie kann man die Einrichtung einer solchen Infrastruktur dann noch gesellschaftlich absegnen? Es wird ja wohl keiner ernsthaft behaupten wollen, daß sich die Menschheit überraschend zum Besseren geändert hätte, sodaß Mißbrauch oder auch nur falsche Behandlung aufgrund technischen Versagens nicht mehr zu erwarten wären.

Es geht also – um auf die Kosten-Nutzen-Abwägung im Status Quo zurückzukommen – nicht um die Aufgabe von ein bißchen Privatheit für ein akzeptables Mehr an Sicherheit und Konsumkomfort. Nein! Weil die technische Infrastruktur von "ein bißchen weniger Privatheit" technisch identisch ist mit der Infrastruktur von "keine Privatheit", geht es schon jetzt um die vollständige, die kategoriale Aufgabe von Privatheit und allen persönlichen Freiheiten, die damit verbunden sind.

Die vielleicht für Einige paradox klingende Konsequenz kann daher eigentlich nur die folgende sein: Jeder demokratische Rechtsstaat, der die Gefahr von totalitären Strukturen als historisches Faktum anerkennt, muß einer Überwachungsinfrastruktur ausschließlich entgegenbauen. Sie darf allerdings in keinem Fall selbst produziert und ausgebaut werden und schon gar niemals perfektioniert werden. Kurz gesagt: Überwachungstechnologie sollte einzig und allein entwickelt werden, um Gegenmaßnahmen gegen ihren Mißbrauch zu produzieren.

Die sich gegenwärtig ausbauende Überwachungsinfrastruktur gestattet rein technisch gesehen also bereits jetzt die totale Überwachung von Handeln und Denken jedes Einzelnen. Das einzige, was potentielle Interessenten davon abhält, sind gegenwärtige Verabredungen auf einen sonst unverbindlichen Status Quo. Die Kosten-Nutzen-Abwägung zwischen ein bißchen Privatheit und ein bißchen Mehr an Sicherheit und Konsumkomfort muß also zusätzlich gegen die in der Zukunft abzuzahlende Hypothek einer sehr, sehr starken Stabilisierung der nächsten Diktatur mitbelastet werden. Und da man (schon gar nicht als Deutscher), die Gefahr einer nächsten Diktatur ausblenden sollte, wird die Rechnung ungleich komplexer.



Fazit

Mit diesen Argumenten hat man nun bessere Karten in der Hand als das bloße individuelle Wertempfinden. Denn keiner kann ernstlich wollen, daß sich eine neue, auf wüsten Internetspekulationen beruhende Klassengesellschaft bildet. Keiner kann wirklich eine in faktischer und geistiger Konformität erstarrte, moralisch-ethisch und in ihren Identitätsformen angsthaft verkümmerte Gesellschaft wollen. Und keiner kann ernsthaft der nächsten Diktatur irgendwo auf der Welt schon jetzt gratis die technischen Mittel der totalen Überwachung von Denken und Handeln aller Menschen in die Hand geben wollen.

All das sind direkte Konsequenzen aktueller Entwicklungen. Es sind sicherlich noch die Anfänge. Aber es sind äußerst faktische Anfänge, keine dystopischen Spekulationen. An diesen jetzt anzusetzen, das ist unsere aktuelle Aufgabe. Und dazu gehören eben – neben den technischen Fakten – auch die präzisen Argumente. Damit jeder weiß, warum die Fakten überhaupt so interessant sind.

Was habe ich eigentlich zu verbergen?

Julian Finn <julian@phinn.de>

Schon im Jahre 1787 hatte der Philosoph Jeremy Bentham die Vision, daß in einem Gefängnis, in dem die Insassen nicht wissen, ob sie überwacht werden, kaum eine Überwachung nötig sei. Schon der Gedanke, daß ein Wärter anwesend sein könnte, würde ausreichen.

Auch als Michel Foucault 1975 das Buch „Überwachen und Strafen" schrieb, hatte er Benthams *Panopticon* im Sinn. Er verglich das allzeit einsehbare Gefängnis mit einer modernen Gesellschaft, die permanente Überwachung als Mittel zur Disziplinierung einsetzt.

Überwachung ist also nur sekundär als Aufklärungsinstrument zu verstehen. In erster Linie ist eine umfassende Überwachung die Grundvoraussetzung einer Gesellschaft, in der sich der Einzelne allen Regeln gegenüber konform verhält. Sie bedeutet auch, daß derjenige, der die Regeln vorgibt, ein Vielfaches an Macht erhält. Schon der Wunsch, etwas daran zu ändern, kann als Auflehnen, als Auffälligkeit betrachtet werden. Der Druck, sich regelkonform zu verhalten, steigt also und wird zur Gefahr für eine offene Gesellschaft. Denn dort, wo Freigeister und Querdenker in die Enge getrieben, wo es schwierig wird, Kritik zu üben, da ist auch eine Weiterentwicklung der Gesellschaft unvorstellbar. Wo kritische Literatur oder Musik, wo progressive Gedanken nicht mehr ohne Angst konsumiert werden können, kann auch keine Demokratie gelebt werden.

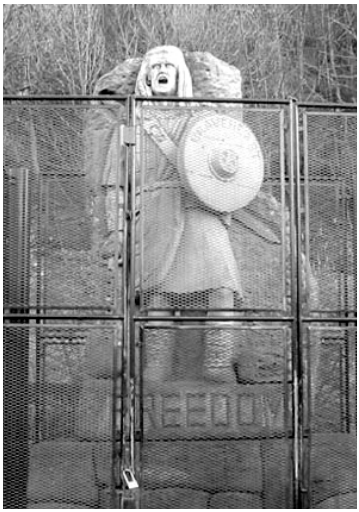
Doch wo fängt diese Gefahr an? Sind denn die paar Kameras auf öffentlichen Plätzen oder die paar Datenbanken wirklich ein Problem?

Wer heutzutage manche Wohnbezirke besucht oder auch einfach nur einkaufen will, wird in großen Lettern damit begrüßt, daß er nun im Dienste der Sicherheit gefilmt wird. Ob er möchte oder nicht: Wenn er den Bezirk betritt, ist er unter konstanter Beobachtung. Wer in den USA ein Flugzeug besteigen möchte, wird freundlich darauf hingewiesen, daß er sich keiner Durchsuchung unterziehen muß, solange er am Boden bleibt – von echter Freiwilligkeit kann hier keine Rede sein.

Auch die Sammelwut an persönlichen Daten nimmt zu: biometrische Reisepässe, DNA-Datenbanken, Telekommunikationsdaten. Alles wird mit Hinweis auf die nötige Aufklärung und Prävention vor Terrorismus und Kriminalfällen generiert, sortiert und gespeichert. Zudem geben Millionen Menschen täglich freiwillig Auskunft darüber, was sie tun oder kaufen. Allein Procter & Gamble kann auf 240.000 Jugendliche vertrauen, die gern dafür, daß sie alle paar Monate ein Parfümpröbchen gratis bekommen, Auskunft über ihre Konsumgewohnheiten geben.

Es ist aber nicht nur die freiwillige oder unfreiwillige Auskunft über persönliche Daten, der biometrische Personalausweis, die Flugpassagierdatenübermittlung oder der freiwillig ausgefüllte Konsumverhaltenfragebogen für das Großunternehmen: ein Klick, ein Bild – Daten entstehen. Daten, deren Umfang man zwar überblicken kann, deren Ziel aber unbekannt ist. Normalerweise weiß man nicht, wo die übermittelte Information gespeichert wird. Es ist unbekannt, ob Verknüpfungen zu anderen Daten geschaffen werden, ob und wie oft Back-ups erstellt und wie diese gelagert und transportiert werden. Sobald diese Daten Browser, Telefon oder Wohnung verlassen, gehören

sie zwar vor dem Gesetz noch ihrem Urheber, faktisch aber sind sie anderen zugänglich und damit jeglicher Kontrolle entzogen. Das gleiche gilt natürlich für alles, was indirekt Auskunft gibt: ein Foto, ein Standort, den das Mobiltelefon übermittelt, Geld, das vom Automaten abgehoben wird.



Das ist in der analogen Welt anders. Wollte man bislang ein Foto auf fünfzig Abdrucke limitieren, vernichtete man danach unter Aufsicht eines Notars das Negativ und konnte somit belegen, daß keine weiteren perfekten Kopien des Bildes entstehen werden. Heute, da Fotolabore längst digital arbeiten, ist das nicht mehr möglich. Niemand weiß, ob nicht irgendwo noch ein digitaler Abzug des Bildes archiviert wurde. Was in diesem Fall noch recht abgehoben klingt, schließlich genügt mir normalerweise die Aussage des Fotolabors, daß keine Kopien erstellt wurden, ist an anderer Stelle durchaus ein Problem. Wer seinen Account bei einem dieser schönen neuen Online-Dienste löscht, kann sich nicht sicher sein, ob die Daten tatsächlich weg sind. Back-ups werden gespeichert, möglicherweise über Jahre aufbewahrt oder bei einem Verkauf der Firma weitergegeben. Unvorsichtige oder voyeuristische Admins werfen vielleicht eines Tages ebenjene Bänder mit dem Jugendsündenfoto in den Müll, von wo aus sie nicht zwingend in der Verbrennungsanlage landen. Oder sie packen die Daten gleich in ein anonymes Blog. Allein die Geschichten über abhanden gekommene Kreditkartendaten würden den Umfang dieses Artikels sprengen. Und während eine Kreditkarte noch gesperrt werden kann und im Zweifelsfall die Bank für den Verlust des Geldes aufkommen muß, gibt es nur selten jemanden, der sich für den Verlust von Privatsphäre zur Verantwortung ziehen läßt.

Daten kumulieren also. Sie werden nicht weniger und verändern sich nicht, auch wenn man selbst längst mit seinem Leben fortgeschritten ist. Jeder kennt das seltsame Gefühl, wenn man nach zehn Jahren einem alten Bekannten begegnet, der inzwischen ein völlig anderer Mensch geworden ist. Die betretene Stille, die entsteht, wenn man einfach nicht mehr weiß, was man sich erzählen soll. Es ist schwer vorstellbar, daß Erinnerungen, etwa an einen romantischen Abend im Park, nicht mehr nur im Gedächtnis oder dem eigenen Fotoalbum, sondern auch in der digitalen Sphäre lagern und eines Tages wieder an das Licht der Öffentlichkeit geraten könnten – daß Maschinen eben kein Auge zudrücken können, sich nicht darauf berufen, daß „das alles schon so lange her“ sei. Nun muß dieser romantische Abend nicht einmal im eigenen Flickr-Account existieren, den man vielleicht damals online mit seiner Fernbeziehung geteilt hat. Schon das Versenden einer E-Mail mit persönlichen Inhalten generiert Kopien dieses einen Bildes, die sich außerhalb der Kontrolle derjenigen befinden, für die sie bestimmt waren.

Hinter den Maschinen, die all das speichern, sitzen Menschen wie du und ich. Menschen, die auch mal das Bedürfnis haben, einen heimlichen Blick in fremde Badezimmerschubladen zu werfen. Beamte, die aus der gleichen Sensationsgier, aus der sie täglich die „Bild“-Zeitung lesen, auch „mal schauen“ könnten, wer aus dem Bekanntenkreis denn so im örtlichen Sex-Shop einkaufen geht oder was der Nachbar so an Musik hört, wenn er allein ist. Der Grund, warum genau diese Daten nicht für jedermann bestimmt sein sollten, ist der gleiche, aus dem mein Nachbar eine zwei Meter hohe Hecke um sein Grundstück gezogen hat und aus dem ich niemandem erzähle, daß ich heimlich die „Sängerin“ Blümchen mag: weil es niemanden etwas angeht – ob es Videobilder sind oder die eigent-

lich nur für meinen Freundeskreis bestimmten Bilder vom Fußballabend.

Doch was, wenn nicht nur der alltägliche Voyeurismus, sondern echte Interessen dahinterstehen? Wenn Staat oder auch Industrie aus ihren eigenen Gründen systematisch in die Privatsphäre eines Menschen eindringen wollen? Einkaufsgewohnheiten, Wohnort, Hobbies und die finanzielle Situation sagen schon viel über einen Menschen, seine möglichen gesundheitlichen Risiken oder seine Zuverlässigkeit aus. Es ist nicht schwer, mit der Kombination einiger weniger Daten Rückschlüsse auf einen Menschen zu ziehen, die möglicherweise voreilig sind, im seltensten Falle aber zum Vorteil des Einzelnen gereichen. Vielleicht ist derjenige, der jede Woche drei Kästen Bier kauft, ein Alkoholiker, vielleicht ist er aber nur spendabel und lädt jeden zweiten Abend ein paar Freunde ein, vielleicht hilft er dem Alkoholiker in seinem Aufgang, der schon zu alt zum Kistenschleppen ist. Die Krankenkasse würde sich wahrscheinlich auf ersteres festlegen und den spendablen Freund oder hilfsbereiten Nachbarn in die Risikogruppe stecken.

Es muß nicht der Alkohol- oder Tabakkonsum sein, der solche Vermutungen zuläßt. Ein häufiger Besucher von Snowboard-Foren wird wahrscheinlich selbst am Sport interessiert sein, ein Abonnent mehrerer Freeclimbing-Newsletter hat vielleicht zumindest vor, selbst einmal ein paar Felsen zu besteigen. Doch was, wenn die Sportunfallversicherung oder der Arbeitgeber sich dafür interessieren? Was, wenn die Staatsanwaltschaft gerade nach einem Menschen fahndet, der einen Mord mit einem Eispickel begangen hat? Sie wird es sich nicht nehmen lassen, auch in der Klettercommunity eine Rasterfahndung durchzuführen. Wer aus dieser Gruppe in letzter Zeit einen neuen Eispickel gekauft hat, wird verdächtig. Egal, ob er damit lediglich zum Eisklettern in die Alpen wollte oder vielleicht sogar nur gern mit seiner Ausrüstung angibt, die er eigentlich noch nie benutzt hat.

Noch dramatischer wird es natürlich, wenn DNA- und Fingerabdruckdatenbanken oder gar gesichtserkennende Kameras existieren. Ein unachtsam weggeworfener Zigarettenstummel – natürlich mit Speichelspuren des Rauchers – in der Nähe des Waldstücks, an dem ein kleines Mädchen verschwindet. Dazu eine Kamera, die am Ortsausgang etwa eine halbe Stunde vor der Tatzeit das Gesicht des Waldspaziergängers aufnimmt: Und schon gilt er als verdächtig.

Dabei muß festgehalten werden, daß Datenbanken und Maschinen eben nicht nach Korrektheit, sondern vor allem nach Plausibilität suchen. Daß mit der Unterstützung von Maschinen der Druck entsteht, sich auf diese zu verlassen. Überwachungskameras verhindern nicht, daß Menschen in U-Bahnhöfen überfallen werden. Aber wenn die Kameras da sind, ist es ein Leichtes, sich darauf zu berufen und das Wachpersonal abzubauen. Wenn dank DNA-Datenbank und Bilderkennung eine Mordkommission nur noch aus drei statt sechs Beamten besteht, spart das möglicherweise Geld. Die Chance, daß der „Schuldige“ aber dank eines Computer-Fehlurteils ermittelt wird, ist in jedem Falle höher.

Was habe ich also zu verlieren? Auch der ständige Druck, unter Verdacht zu stehen oder geraten zu können, führt zu schon genannter Verhaltensänderung. Auch wer nicht sofort davon ausgeht, daß all seine Daten verkauft, zusammengeführt und gegen ihn verwendet werden, wird schon bald unter dem ständigen Eindruck der Überwachung beginnen, sich anders zu verhalten. Ob es nur das Quentchen mehr an Verschlossenheit ist, das man beim Vorstellungsgespräch an den Tag legt (und das vielleicht genau deshalb zur Absage führt), oder das eine Bier weniger, das man trinkt, um nicht die videoüberwachte Straße herunterzutorkeln. Vielleicht ist es auch nur die eine Blümchen-CD, die ich nicht kaufe, weil mein Nachbar davon erfahren könnte. Überwachung und Datensammelei gehen Hand in Hand. Sie arbeiten gemeinsam daran, daß Privatsphäre zur Seltenheit wird, möglicherweise auch zum Luxusgut, das sich nur wenige leisten können. Daran, daß Stück für Stück die Grundfesten unserer Individualität untergraben werden. Und gegen die Vielfalt, die eine freie und offene Gesellschaft ausmacht.

Das anonyme Preisausschreiben "Keine Macht für niemand"

<46halbe@weltregierung.de> und <erdgeist@erdgeist.org>

Wir dürfen hocherfreut mitteilen, daß es einen Gewinner des anonymen Preisausschreibens gibt! Wir können leider natürlich nicht sagen, wie er oder sie heißt. Wir veröffentlichen aber gern die Antworten. Falls es dazu Kommentare gibt, freuen wir uns, diese in der Leserbriefsektion abdrucken zu können. Bitte wie immer an ds@ccc.de senden.

An dieser Stelle nochmal einen herzlichen Dank allen Einsendern!

1.) Du bist in einem offenen Funknetz. Nenne drei praktische Wege, wie jemand dich tracken könnte!

a) Jemand hört den Netzwerkverkehr mit einem passiven WLAN-Sniffer ab und ordnet die Datenpakete mit Hilfe der MAC-Adresse zu.

b) Der Betreiber des Funknetzes schneidet den Verkehr mit einem gewöhnlichen Packetsniffer mit.

c) Ein Dritter gibt durch gefälschte ARP- oder DHCP-Pakete vor, das Gateway oder der DNS-Resolver des Netzwerkes zu sein und kann so den gesamten Netzwerkverkehr bzw. alle Namensauflösungen verfolgen und manipulieren.

Kommentar der Redaktion: Gern gehört hätten wir auch die einfachere Variante:

d) Dein Tischnachbar im Cafe schaut dir beim Surfen und E-Mails schreiben über die Schulter, der üble Spanner.

2.) Du verwendest deinen Browser für http mit TOR. Nenne drei praktische Wege, wie deine IP dennoch aufgedeckt werden kann! Dabei ist der Angreifer nicht die NSA.

a) Ein Java-Applet, das vom Webbrowser gestartet wird, stellt eine nicht-anonymisierte Verbindung über das Internet her.

b) Ein Flash- oder ActiveX-Objekt oder JavaScript nutzt Funktionalitäten oder Schwachstellen des Browsers, um die IP-Adresse zu ermitteln.

c) Ein Cookie, der beim Besuch einer Seite über eine nicht-anonymisierte Verbindung gesetzt wurde, verrät die IP-Adresse oder sogar die Identität des Benutzers.

Kommentar der Redaktion: Welch unglaubliches Vertrauen in die Neutralität der Infrastruktur. Der Redaktiton brannte noch folgende Antwort unter den Zehnägeln:

d) Der Betreiber der Exit-Node ist nicht so vertrauenswürdig, wie man es eventuell erwartet.

3.) Manchmal nervt dich, daß TOR zu langsam ist. Daher schaltest du ihn zuweilen ab oder benutzt einen Filter für bestimmte Webadressen, die du weiterhin nur mit TOR besuchst. Erkläre, warum du damit deine Anonymität gefährdest!

Beim Besuch der Seite kann ein Cookie gespeichert oder eine Session-ID verwendet werden. Mit deren Hilfe können Seiten-Anfragen eindeutig einem Benutzer zugeordnet und die verwendeten IP-Adressen protokolliert werden. Dadurch wird es möglich, frühere und spätere Anfragen mit der wahren Adresse in Verbindung zu bringen.

Kommentar der Redaktion: Sehr schön. Als Beispiele seien hier ad-Server wie *doubleclick.net* genannt. Weiterdenkend könnte man TOR beschleunigen, indem man in die Infrastruktur Zeit und Geld investiert und selber TOR-Nodes betreibt. Da in der momentanen Situation der Betrieb eines TOR-Exit-Nodes nicht jedermanns Sache ist, kann man alternativ auch Sach- oder Finanzmittel für den Betrieb der CCC-TOR-Server beisteuern. (Wir freuen uns über Post an *torwarte@ccc.de*.)

4.) Du hast JavaScript in deinem Browser aktiviert. Nenne zwei Möglichkeiten, wie dich jemand dadurch tracken kann!

a) Ein Seitenbetreiber bindet über dynamisch per JavaScript erstelltes HTML ein Bild mit entsprechend generierter URL ein, anhand dessen der Betreiber meine Anfragen und weitere per JavaScript verfügbare Informationen protokolliert.

b) Der Betreiber generiert per JavaScript Links, die diverse Systeminformationen enthalten, die bei der Anfrage mit übertragen werden.

Kommentar der Redaktion: Wie sich zeigt, ist das Ausführen einer Turing-vollständigen Sprache im Browser ein Quell kreativer Tracking-Szenarien. Am lustigsten wäre aber sicherlich, auf der Webseite unappetitliche Inhalte zu präsentieren und durch JavaScript das Schließen der Seite zu verhindern. Etwaige kurzfristig und unüberlegt abgesetzte Beschwerden darüber ließen sich sicher tracken.

5.) Erkläre, wie du auf einfachem Wege verhinderst, daß dich jemand mittels JavaScript trakken kann, ohne daß du global die Benutzung von Javascript verbietest!

Man kann das Risiko mindern, indem man dynamisch per JavaScript generiertes HTML in den Browsereinstellungen verbietet. Somit bleibt dem Betreiber nur noch die Möglichkeit, Cookies und serverseitig dynamisch generiertes HTML zu verwenden.

Kommentar der Redaktion: In der Politik ist es übrigens auch ein erprobtes Mittel, sich den Inhalt der Webseite von seiner Sekretärin ausgedruckt vorlegen zu lassen.

6.) Wie kannst du wirkungsvoll verhindern, daß bestimmte Applikationen deine Proxy-Einstellungen umgehen?

Man kann dies verhindern, indem man über einen Paketfilter alle ausgehenden Pakete verwirft oder ablehnt, die nicht vom Proxyserver versendet worden sind.

Kommentar der Redaktion: Man sollte sich solche „bestimmten" Applikationen gar nicht erst installieren. Wenn der Hund aber schon in den Brunnen gepinkelt hat, sind „Personal Firewalls" kein gutes Mittel: Diese sind meist selbst nur mehr schlecht als recht zusammengeschriebene Auswüchse von wirtschaftlichen Sachzwängen ihrer Hersteller.

7.) Nenne vier local services, die deine Identität im local network oder beim VPN-Endpunkt aufdecken können!

a) Ident
b) TAP
c) SMTP
d) NetBIOS

Kommentar der Redaktion:

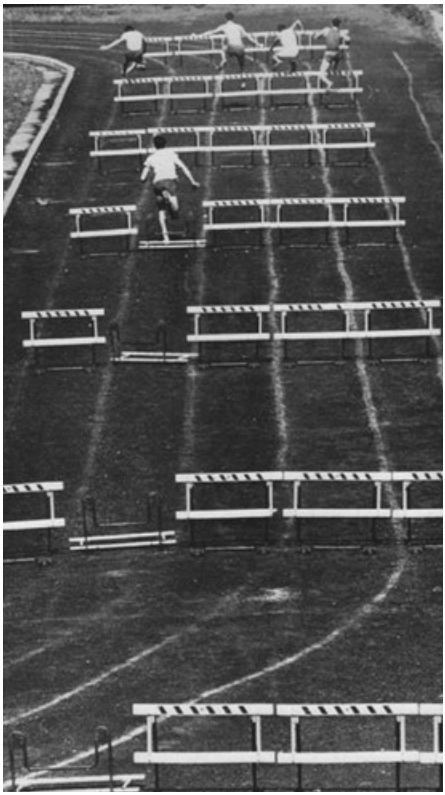
e) http://127.0.0.1:80/~admin/Privatpron/

8.) Die Wikipedia blockiert das Editieren von Artikeln mit TOR. Nenne mindestens zwei Möglichkeiten, wie du diese Blockierung umgehen kannst, ohne deine Anonymität zu verlieren!

a) Einen Benutzer-Account anlegen.

b) Zusätzlich einen offenen Proxy-Server verwenden, der nicht geblockt wird.

Kommentar der Redaktion: Leider ist Antwort a) keine Möglichkeit, um Wikipedia-Artikel zu editieren. In der Regel werden auch Benutzer mit Account geblockt, wenn sie TOR verwenden. Wir beklagen dies. Der Redaktion sind spontan fünf Wege eingefallen, sich vor Vandalismus zu



schützen, ohne das TOR-Netzwerk kaputtzuspielen, diese wurden der Wikipedia Deutschland anonym eingesendet.

9.) Du möchtest einen anonymen Mailaccount haben. Welche Provider sollte man hier nicht verwenden? Begründe, worin jeweils die Gefahr besteht, wenn man diese Provider benutzt!

Man sollte solche Provider vermeiden, die explizit erwähnen, daß sie Anonymität bieten. Sie sind meistens nicht seriös und werden sicherlich Verbindungsdaten vorhalten, um sich rechtlich abzusichern.

Kommentar der Redaktion: Nach dem computergestützten Auflösen der zahlreichen verschachtelten Satzteile kommen wir zu dem Schluß: Honey, name three.

10.) Erkläre, welche Gefahren generell bestehen, unabhängig vom Provider, wenn man einen anonymen Mailaccount klickt!

Selbst wenn man keinen Namen und keine Kontaktadresse angibt, bedeutet dies nicht, daß man anonym ist. Dem Provider ist es immer noch möglich, den Account mit einer IP-Adresse in Verbindung zu bringen.

Kommentar der Redaktion: Tja, man macht sich auch verdächtig. Die Gefahren für der Gesellschaft!!! Anonyme E-Mail wird doch eh nur von Terroristen, Kinderschändern, Hooligans und Nazis benutzt. In welches Licht rückt man sich denn bitte sehr?

11.) Du möchtest einen öffentlichen IRC-Server anonym verwenden. Welche Einstellungen deines Client können hierbei deine Anonymität bedrohen?

Bedroht werden kann meine Anonymität von Einstellungen, die das Client-To-Client Protocol (CTCP) und Direct Client-to-Client (DCC) Transfers betreffen.

Kommentar der Redaktion: Weiter oben wurde ja schon der ident-Service genannt, dessen Fehlen das Einloggen auf dem IRC-Server verhindert. Zusätzlich können Einstellungen, die Smileys und Textfarbe betreffen, Auskunft über dein Geschlecht und deine sexuellen Gewohnheiten geben.

12.) Nenne mindestens zwei anonyme Zahlungswege!

a) Bargeld per Post ohne Angabe der Anschrift des Absenders

b) Zahlungsanweisung (money order)

Kommentar der Redaktion: Antwort a) skaliert leider nicht. Wo sich bei digitaler Bezahlung ein nur dem Geldempfänger und dem -absender bekanntes Geheimnis in den Nachkommastellen verstecken läßt, würde sich dieser Versuch mit Bargeld in unendlichen Komplikationen, hohen Geldbeträgen oder unhandli-

chen Stückelungen niederschlagen. Ab einer bestimmten Geldmenge sehen wir zudem weitere praktische Probleme. Die Antwort besticht aber in der B-Note, darum lassen wir sie durchgehen, sofern kein videoüberwachter Briefkasten verwendet wird. Antwort b), auch als nigerianisches Inkasso bekannt, läßt sich komplett unelektronisch nur in videoüberwachten Bankhäusern umsetzen.

13.) Du möchtest Google Groups verwenden, um im Usenet zu posten. Erkläre, was du vor und nach dem Zugriff beachten mußt?

Vor dem Zugriff sollte man alle Google-Cookies entfernen und anschließend das Tab bzw. Fenster schließen und die Cookies wieder entfernen. So erschwert man, daß frühere oder spätere Anfragen bei Google mit dem Posting in Verbindung gebracht werden.

Kommentar der Redaktion: Man könnte auch darauf verzichten, mit seinem Namen zu unterschreiben. Aber mal Scherz beiseite, gerade Postings zu sehr speziellen Randgruppenthemen lassen sehr leicht auf einen bestimmten Menschen schließen. Im Übrigen ist daneben immer auch eine Textanalyse möglich, um das Geschriebene einer Person zuzuordnen.

14.) Du sitzt hinter einer Firmen-Firewall, die jeden Internet-Zugriff protokolliert und außerdem bestimmte Ports sowie Programme blockiert. Erkläre, wie du trotzdem machen kannst, was du eben so machen willst!

Man kann seinen Netzwerkverkehr über einen verschlüsselten SSH-/VPN-Tunnel leiten.

Kommentar der Redaktion: Ja, aber nur ein **eigener** SSH-/VPN-Tunnel ist ein guter SSH-/VPN-Tunnel.

15.) Du sitzt immernoch hinter besagter Firewall. Nenne drei Dinge, die dein Antrieb sind, die Firewall zu umgehen!

a) Ich mag es nicht, wenn jemand meine Freiheit einschränkt.

b) Ich lege sehr viel Wert auf meine Privatsphäre und lehne es ab, daß andere meinen Netzwerkverkehr mitlesen.

c) Ich bin der Überzeugung, daß ich ein Recht auf beide (also die Freiheit und die Privatsphäre) habe.

Kommentar der Redaktion: Also naja, etwas konkreter hätten wir es ja doch gern gehabt. *hust* Nix YouPorn, nix Videochatten mit der oder dem Liebsten? Nicht mal eBay während der Arbeitszeit?

16.) Du bist weiterhin in der Firma mit der vordergründig restriktiven Firewall. Du weißt, daß der dortige Netzwerk- und Firewallverantwortliche mittels eines Keyloggers auch deine Tastatureingaben überwacht. Du mußt aber ganz dringend deiner Mama tausend Euro überweisen. Erkläre, wie du das Paßwort für dein Online-Banking so eingibst, daß dieser Schnüffler leer ausgeht!

Ich starte eine Bildschirmtastatur, um dem Keylogger zu entgehen und verbinde mich per SSH zu meinem Shell-Server. Dort starte ich den Textbrowser, um über das barrierefreie Webinterface meiner Bank die Überweisung zu tätigen.

17.) Erkläre, wie man auf einfachem generischen Weg ein verstecktes Rootkit auf einem Rechner aufdeckt!

Man sucht mit einem Port-Scanner nach lauschenden Programmen. Man untersucht den Netzwerkverkehr des Rechners mit einem Sniffer.

Kommentar der Redaktion: Der generische Weg wär eigentlich, die Kopie der Festplatte zu nehmen und einen anderen Rechner zur Betrachtung des Dateisystems zu verwenden.

18.) Gib zwei Beispiele, warum der Online-Kauf von Büchern gefährlich sein kann!

a) Man gibt einem großen Unternehmen persönliche Vorlieben preis, die dieses eigennützig verwenden könnte.

b) Man muß seine Kreditkartendaten oder Bankverbindung übermitteln und erteilt dem Unternehmen eine Einzugsermächtigung.

Kommentar der Redaktion: ...oder man wird bei nächsten Versuch, ein Flugzeug zu besteigen, gebeten, doch bitte erstmal mitzukommen...

19.) Du möchtest trotzdem ein Buch online kaufen. Erkläre, wie du vorgehst, wenn du die eben genannten Gefahren ausschließen willst!

a) Ich teile mir einen Account mit vielen Leuten.

b) Ich verwende die Anschrift eines Vereins oder einer Firma.

c) Ich bezahle nur auf Rechnung oder per Nachnahme.

Kommentar der Redaktion: Wir bitten bei dieser Gelegenheit, davon Abstand zu nehmen, Bücher an die Postadresse des CCC zu senden. Ausnahmen sind natürlich Geschenke oder etwaige Schriftstücke, die aufgrund ihres brisanten Inhalts an uns geschickt werden.

20.) Wie kannst du, im Falle du das Quiz gewinnst, sicherstellen, daß du den Preis von uns bekommst, ohne deine Anonymität preiszugeben? Zeige mindestens drei Wege auf, unter der Bedingung, daß in keinem der Szenarien die physische Integrität eines Mensches gefährdet wird!

a) Die Antworten signiere ich mit einem PGP-Key, den ich nur für das Preisausschreiben erstelle. Anschließend verschlüssele ich die Nachricht mit dem public key der Redaktion und sende sie per TOR anonymisiert an ds@ccc.de. Sollte ich das Preisausschreiben gewinnen, muß ein Mitglied der Redaktion den Preis in einem Bahnhofschließfach deponieren und den Schlüssel an einem Ort hinterlassen, der – mit meinem public key verschlüsselt – in der nächsten Datenschleuder bekannt gegeben wird.

b) Ich wähle eine zufällige Anzahl Leute aus dem CCC-Umfeld aus, die vertrauensvoll sind, aber die ich nicht direkt kenne, und besorge mir deren public keys. Anschließend verschlüssele ich ein paar Zufallsdaten mit meinem richtigen PGP-Key, dann mit dem ersten Key, anschließend mit dem zweiten, dem dritten, und so weiter. Diese Nachricht lege ich meiner – wie oben anonymisiert zugestellten – Antwortmail bei und bitte darum, den gewonnenen Preis an die Person auszuhändigen, für welche die Nachricht zuletzt verschlüsselt wurde. Diese entschlüsselt die Nachricht und erfährt den Namen der nächsten Person in der Kette und gibt den Preis sowie die entschlüsselte Nachricht weiter, sodaß diese Person ihrerseits die nächste Schicht der Nachricht entschlüsseln kann, bis der Preis irgendwann bei mir angelangt ist. Da niemand weiß, daß ich die letzte Person in der Kette bin, bleibe ich anonym.

c) Die letzte Methode läßt sich auch um die Zustellung per Post über verschiedene Länder erweitern, wobei ich das Geld für die enormen Versandkosten der Redaktion per money order zukommen ließe.

Kommentar der Redaktion: Na? Hast du den Preis schon bekommen oder hat einer deiner „Freunde“ das Teil behalten?

Suchmaschinen, Privatsphäre und andere Illusionen

Frédéric Phillip Thiele und Henrik Speck

You have zero privacy anyway. Get over it. – Scott McNealy, CEO of Sun Microsystems

Der Trend zur Datenprostitution ist nicht zu übersehen. Die mehr oder weniger aktive Beteiligung an der Kompromittierung der Privatsphäre hat einen Höhepunkt in den Generationen von Schülern und Studenten gefunden, die sich öffentlich in verschiedenen sozialen Netzwerken und Weblogs entblößen. Weitere Verschiebungen der Privatsphäre entstehen durch die Unzahl verschiedener Dienste und Plattformen, die durch die Preisgabe vermeintlich weniger privater Daten komplette Nutzungsprofile, Klick- und Kaufverhalten, Nutzerinteressen und Kommunikationsprofile erstellen können. (Meusers 2006)

Daß die Transformationen im Verhältnis von öffentlichem und privatem Raum gesellschaftlich noch nicht vollständig nachvollzogen sind, wird durch das inkonsequente Verhalten vieler Internetnutzer deutlich: Obwohl die freiwillige Herausgabe von persönlichen Informationen, Namen, Adressen, Bankverbindungen und Kommunikationsverhalten mittlerweile gesellschaftsfähig geworden ist, demonstrieren viele Internetnutzer eine kaum erklärbare Scheu beim Umgang mit anderen Metaebenen – insbesondere beim Einkommen, Vermögen, Verschuldungsgrad und innerhalb von Patientenkarteien wird versucht, die Illusion der Privatsphäre aufrechtzuerhalten. Dies gilt auch für die an der Gesetzesfindung beteiligten Abgeordneten, die sich einer Offenlegung ihrer Gehälter standhaft verweigert hatten.

Diese Versuche sind selbstverständlich rein kosmetisch, schon bei der Einreise in befreundete Länder wird eine Kompletterfassung einschließlich Fingerabdrücken und Mugshots freundlich begrüßt. Laptops, Festplatten und andere Datenträger können, wie ein US-amerikanisches Gericht im Juli 2007 bestätigte, dabei komplett auseinandergenommen und einer forensischen Analyse unterzogen werden ohne entsprechenden Grund, Verdacht oder Gerichtsbeschluß – die Ausnahmeregelungen zu den Grenzkontrollen bereiten dafür den rechtlichen Hintergrund. Zusammen mit den in den Reisepässen enthaltenen biometrischen Informationen entstehen damit interessante Diskussionsbeiträge für die sogenannten Screener, die sich zumeist am Boden der Gehaltsgruppen bewegen. (Sharkey 2006)

Einige besonders interessante Veränderungen der Privatsphäre werden von *attrition.org* verwaltet, die seit dem Jahrtausendwechsel in ihrem „Data Loss"-Verzeichnis die Eigentümerwechsel von Nutzerdaten dokumentieren. Die Anzahl der dabei kompromittierten Nutzerprofile ist ständig ansteigend und beträgt momentan mehr als 100 Millionen. (Attrition, Zeller 2006a und 2006b)

Kevin Poulsen verwies dabei insbesondere auf die kompromittierten 800.000 Profile der Universität von Kalifornien, die 130.000 der Firma Aetna und die 382.000 Nutzerdaten und Social Security Numbers, die beim Flugzeughersteller Boeing betroffen wurden, als er das traurige Ausmaß dieser Veränderungen kommentierte. Poulsen muß es wissen: Er ist eine Hacker-Ikone. Im Juni 1994 bekannte er sich unter dem Druck der US-Regierung des Computermißbrauchs, der Geldwäsche und der Behinderung der Justiz schuldig und wurde zu 51 Monaten Haftstrafe und 56.000 US-Dollar Strafe verurteilt. Zu diesem Zeitpunkt war dies die härte-

ste Strafe, die bis dahin für Hacken vergeben wurde. Er wurde durch den Vorläufer des Web 2.0, die Fernsehsendung Unsolved Mysteries – eine amerikanische Variante von „XY Ungelöst" – aufgespürt und verbrachte tatsächlich drei Jahre im Gefängnis. Für drei weitere Jahre war es ihm durch das Gericht verboten, einen Computer zu benutzen.

Diese Zeiten sind längst vorbei: Poulsen arbeitet jetzt für das „Wired Magazine" und demonstrierte im Oktober 2006, wie sich durch primitive Datenabgleiche Sexualstraftäter identifizieren lassen, die innerhalb des sozialen Netzwerkes „MySpace" auf Opferjagd gehen. Durch Poulsens Arbeit konnten 744 verurteilte Sexualstraftäter innerhalb des (US-amerikanischen) MySpace-Netzwerkes identifiziert werden – eine Person, Andrew Lubrano, wurde daraufhin verhaftet. (Poulsen 2006)

Die Veränderungen, die sich aus der Verletzung der individuellen Selbstbestimmung ergeben, sind insbesondere für die Opfer von Identitätsbetrug schmerzlich. Die New York Times hat diesem Thema bereits mehrfach ganze Artikelserien gewidmet. (New York Times 2005)

Insbesondere der Umgang mit derartigen Transformationsprozessen ist Grund zur Besorgnis: Für viele Firmen entspricht die öffentliche Bekanntgabe derartiger Unfälle einem Offenbarungseid. Die Mehrzahl zieht es deshalb vor, ihre Kunden nicht oder nicht in angemessenem Umfang zu informieren. Den Kunden wird dabei insbesondere das Ausmaß und die Details der kompromittierten Daten verschwiegen. Die wenigen Nachrichten liefern meist keine brauchbaren Informationen zu den möglichen Konsequenzen beziehungsweise welche Schritte durch den Verbraucher zur Schadensminimierung unternommen werden können. Für eine große Anzahl der betroffenen Kunden sind derartige Vorgänge damit nicht nachvollziehbar. (Sullivan 2005)

Digitale Jäger und Sammler

Die bereits beschriebenen Erscheinungen verblassen im Vergleich zu den Datenerhebungsmöglichkeiten durch Suchmaschinen. Suchmaschinen agieren als Gralshüter der Wissensgesellschaft. Sie ermöglichen einen Zugriff auf die ständig anwachsenden Inhalte des Internet, sie werden von einem Großteil der Internetnutzer als Navigationsersatz benutzt, ein Ansteigen der Nutzungsintensität und Häufigkeit ist seit Jahren zu beobachten.

Diese zentrale Funktion erlaubt es Suchmaschinen, auch Nutzerprofile in einer Komplexität zu erstellen, welche die Staatsicherheit der DDR als Kinderschutzbund erscheinen läßt. In den sogenannten Logfiles werden bei jeder Suche und bei jedem Klick innerhalb der Suchergebnisse nicht nur transaktionsbezogene Daten, zum Beispiel Datum, Uhrzeit, besuchte Webseite, Suchwörter erhoben, sondern auch spezifische Accountinformationen, die zum Beispiel den Browsertyp, Version, Betriebssystem, Sprache und IP-Adresse beinhalten. Gekoppelt mit den Nutzeraccounts der verschiedenen Dienste, die durch kleine Tracking-IDs, sogenannte Cookies, identifiziert werden, ergibt sich insbesondere bei längerfristiger Nutzungsdauer das Abbild eines gläsernen Bürgers. Die durch Datenschutzgesetze vorgeschriebene informationelle Selbstbestimmung wird dadurch unterlaufen, daß wie im Fall von Google die Cookies praktisch nie verfallen (erst im Jahr 2038) oder aber dadurch, daß die entsprechenden

Keine Anzeige

Löschanforderungen – im klaren Gegensatz zu den sonst so benutzerfreundlichen Angeboten – mit besonderer Sorgfalt tief in den Abgründen der Suchmaschinen versteckt werden.

Die durch die Suchmaschinen gesammelten Daten erhalten insbesondere dadurch an Brisanz, da hier auch Nutzerprofile erhoben werden und somit nachverfolgt werden können, die zum Beispiel für Strafverfolgungsbehörden eine richterliche Verfügung voraussetzen. Durch die Verlagerung auf private Unternehmen, insbesondere wenn diese sich wie alle führenden Suchmaschinenanbieter im Ausland befinden und damit außerhalb der Reichweite national geltender Datenschutzrichtlinien, können vernachlässigbare Einschränkungen, insbesondere innerhalb des demokratischen Rechtsverständnisses, erfolgreich unterlaufen werden. Welche Relevanz diesen Daten zukommt, zeigte das Vorgehen der US-Regierung im Frühjahr 2006, als von den Marktführern im Suchmaschinenbereich (Google, Yahoo, MSN und AOL) die Herausgabe umfangreicher Logfiles der Suchanfragen verlangt wurde. Während Yahoo, MSN und AOL sich widerstandslos der Justiz beugten, protestierte Branchenführer Google getreu dem Firmenmotto „don't be evil" gegen die Herausgabe der Daten. Die US-Generalstaatsanwaltschaft reichte darauf beim US District Court for the Northern District of California eine Klage gegen Google auf Herausgabe der Daten ein. (Hafner 2006)

Ob Google wirklich die Privatsphäre der Nutzer am Herzen lag oder ob es sich vielmehr um einen geschickten Schachzug der Marketingabteilung zur Aufbesserung des Firmenimage handelte, bleibt dabei unbeantwortet. Der Patriot Act der Vereinigten Staaten verpflichtet auch Suchmaschinenbetreiber zur sofortigen Herausgabe angeforderter Informationen. Die betroffenen Firmen sind weiterhin verpflichtet, über diese Vorfälle zu schweigen.

Das AOL-Vorkommnis

AOL Research veröffentlichte im August 2006 eine frei verfügbare Datenbank mit 20 Millionen Suchanfragen von 658.000 AOL-Nutzern im Internet, die detaillierten Nutzerprofile wurden dabei durch simple Nutzer-IDs ersetzt. Die angestrebten Forschungsinteressen wichen schnell der öffentlichen Aufregung. Wenige Tage nach der Veröffentlichung der Daten wurden diese bereits wieder vom Netz genommen. Chefentwicklerin Maureen Govern mußte ihren Arbeitsplatz räumen, und AOL schloß die gesamte Forschungsabteilung. (Karnitschnig 2006)

Trotz aller Bemühungen, den brisanten Datensatz möglichst schnell wieder verschwinden zu

lassen, verbreitete sich dieser innerhalb weniger Tage in einschlägigen Blogs und Foren. Bereits nach einigen Stunden wurden erste Analysen des Datenmaterials einschließlich der beinhalteten Nutzerprofile im Internet veröffentlicht. Neben statistisch interessanten Daten über das Suchverhalten der Suchmaschinennutzer offenbart diese Datensammlung noch weitaus brisantere Details. So enthält der Datensatz auch Kreditkartennummern, Sozialversicherungsnummern, Paßwörter und E-Mails und eine ganze Reihe weiterer, teils sehr skurriler, teils erschreckender Details.

Obwohl die Suchanfragen von AOL in einer anonymisierten Form herausgegeben wurden, die keinen direkten Zugriff auf Nutzernamen oder IP-Adressen ermöglichte, lassen sich durch den Umfang des Datenmaterials in vielen Fällen individuelle Nutzer anhand ihrer Suchanfragen identifizieren. Die bereits in mehreren Forschungsarbeiten untersuchten Vorstellungen von Privatsphäre und Anonymität im Internet erscheinen nur illusorisch. (Speck 2004)

Diese Problematik griff auch die New York Times auf. So enttarnte die Zeitung den Nutzer hinter der User-ID 4417749 anhand der gestellten Suchanfragen. Darunter befanden sich Anfragen wie „numb fingers“, „60 single men“ oder „dog that urinates on everything“. Eine kurze Recherche des Suchportfolios verriet auch die wahre Identität des Suchenden. Dabei handelte es sich um die 62-jährige Thelma Arnold aus Lilburn im US-Bundesstaat Georgia. Die ältere Dame verriet ihre Identität durch Suchanfragen wie „landscapers in Lilburn, Ga“, „homes sold in shadow lake subdivision gwinnett county georgia“ und Suchen nach verschiedenen Personen mit dem Nachnamen „Arnold“. So war es für die Journalisten der New York Times ein Leichtes, die Dame ausfindig zu machen. Konfrontiert mit der Veröffentlichung ihrer Suchergebnisse zeigte sich Ms. Arnold sehr empört („We all have a right to privacy“) und kündigte an, AOL zukünftig den Rücken zu kehren. (Barbaro 2006)

Dabei wählte die New York Times bewußt eine Person mit einem besonders harmlosen und unverfänglichen Suchprofil. Die Suchanfragen offenbaren oftmals intime Details, Sorgen und Befürchtungen. Sexuelle Vorlieben, gesundheitliche Probleme, politische Ansichten oder die finanzielle Situation stellen dabei nur die Spitze des Eisberges dar. Manche Suchhistorien erzählen sogar ganze Lebensgeschichten. Eine Untersuchung der Suchanfragen offenbart menschliche Abgründe: Allein die Häufung von Suchanfragen wie „how to kill your wife“ und „child porn“ sind erschreckend. (AOL Data Collection)

Welch detaillierte Nutzerprofile sich anhand der Suchanfragen erstellen lassen, sind leicht am zufällig ausgewählten AOL-Nutzer mit der User-ID 1588208 zu verdeutlichen. Dieser Nutzer plant einen Urlaub in Orlando, Florida, wo er gern die Universal Studios besuchen möchte. Nach Orlando möchte er mit der Fluggesellschaft JetBlue fliegen, wobei er leider noch nicht die passenden Koffer für seinen Flug hat und daher sehr interessiert an den Produkten der Firma AmericanTourister ist.

Auch über den gesundheitlichen Zustand unseres Nutzers gibt das Suchprofil Auskunft. So scheint unser Nutzer sein rechtes Bein verloren zu haben. Eine Vielzahl von Suchanfragen zum Thema Schuhkauf von speziellen orthopädischen linken Schuhen zeigt, daß der Schuhkauf für unseren Nutzer auch nicht ganz einfach ist.

Sportwagen und Boote scheinen ebenfalls in das Interessensgebiet des Nutzers zu gehören. Besonders ein Chrysler Crossfire, ein Porsche Cayman, eine Chevy Corvette oder ein BMW haben es ihm angetan. Weiterhin scheint unser Nutzer auch an der Finanzierung einer Eigentumswohnung interessiert zu sein, und auch das Pay-TV-Angebot von Verizon hat sein Interesse geweckt.

Doch die Interessen unseres Nutzers liegen auch in anderen Bereichen. So bezieht sich der überwiegende Teil der Suchanfragen auf eindeutig pornographische Inhalte. Seine besonderen Vorlieben liegen hier bei College Girl und Celebrity Tapes von Pamela Anderson bis Britney Spears.

Profiler

Schon eine derart oberflächliche Analyse des Suchprofils liefert einen tiefen Einblick in die Privatsphäre des Nutzers und erlaubt eine recht genaue Vorstellung von der Person hinter der anonymen User-ID 1588208. Dabei handelt es sich bei dem ausgewählten Fall um keinen Sonderfall. Das Suchprofil eines jeden Nutzers wird einen ähnlich detaillierten Einblick bieten. Hinzu kommt, daß sich jedes Profil mit jeder neuen Suchanfrage immer weiter verdichtet. Wie ein Puzzle fügt sich das Gesamtbild mit jedem Einzelteil immer weiter zusammen.

Die Auswertung der Nutzerprofile erfolgt dabei längst nicht mehr manuell, entsprechende Algorithmen erlauben eine Klassifizierung und Clusterung anhand einer Vielzahl von Eigenschaften. Zwar geben alle großen Suchmaschinen an, daß keinerlei personalisierte Analyse der Suchanfragen durchgeführt wird und daß die Daten der Nutzer nicht an Dritte weitergegeben werden, dennoch stellt sich hier die Frage, wie seriös diese Versprechungen zu bewerten sind.

Der kommerzielle und der politische Wert solch detaillierter Profile ist nicht von der Hand zu weisen. Auch der Bereich des Online-Marketings entwickelt sich immer weiter weg von ungenauer Massenwerbung hin zu zielgruppenspezifischen Werbeformen. Hier liegt das eigentliche Geschäftsmodell der Suchmaschinen: Wer wie Google 99% seines Einkommens mit Werbung erzielt, kann den Profit nicht unerheblich steigern, je genauer die Werbung auf die Zielgruppe abgestimmt wird. Dabei erweist es sich durchaus als förderlich, daß Suchmaschinen durch ihre vielen Kooperationen und Zusatzdienste weitere Informationsquellen zur Verfügung haben. Selbst hartnäckige Suchmaschinenverweigerer sind durch die von den Suchmaschinen auf Webseiten angebotene Werbung verfolgbar; integrierte E-Maildienste erlauben die Erfassung des Kommunikationsverhaltens und des sozialen Netzwerkes; Preissuchmaschinen und elektronische Bezahlverfahren erlauben Einblicke in das Finanzverhalten; Browsertoolbars verfolgen jede Surfsession; Desktopsuchmaschinen können sich eines Tages als dankbare Dienstleister für Strafverfolgungsbehörden und Interessenverbände der Film- und Musikindustrie erweisen. (Speck 2005)

Betrachtet man den Nutzer mit der User-ID 17556639, der mit Hilfe der Suchmaschine nach Möglichkeiten sucht seine Frau umzubringen, so könnte das Suchprofil schnell zum Täterprofil werden. Selbst eine Vorhersage von Straftaten anhand einer Analyse der Suchmaschinenanfragen scheint damit nicht ausgeschlossen. Assoziationen zu Szenarien, wie sie in Steven Spielbergs Film „Minority Report“ beschrieben werden, erscheinen dabei nicht unmöglich. (Minority Report 2002)

Scotland Yard hat seine Pläne bereits zur Diskussion gestellt: Britische Polizeipsychologen versuchen, eine Datenbank mit möglichen Tätern anhand ihrer psychologischen Profile aufzubauen, bevor sie ihre Verbrechen begehen. Angestrebt wird hierbei eine Klassifizierung der Bürger nach Bedrohungspotentialen. Stillschweigend wird dafür die Profilierung und Bespitzelung von Millionen unschuldiger Bürger vorausgesetzt – sofern man innerhalb dieses verschobenen Sicherheitsverständnisses überhaupt noch von Schuld reden kann. Die Unschuldsvermutung muß dafür sicherlich ausgesetzt werden. (Cowan 2004, Agence France-Presse 2006, Bannermann 2006a und 2006b)

Ein frohes neues Jahr.

Bibliographie

Agence France-Presse. „Prävention Durch Profiling. Scotland Yard plant Datenbank der künftigen Mörder." Spiegel. November 27, 2006:
http://www.spiegel.de/panorama/justiz/0,1518,451021,00.html

AOL Data Collection.
http://www.aoldatacollection.com/

Attrition.org Data Loss Archive and Database:
http://attrition.org/dataloss/

Bannerman, Lucy. „The woman who aims to spot killers before they can strike." The Times. November 27, 2006:
http://www.timesonline.co.uk/article/0,,200-2473247,00.html (2006a)

Bannerman, Lucy. „Police target dangerous suspects before they can offend." The Times. November 27, 2006:
http://www.timesonline.co.uk/article/0,,2-2473501,00.html (2006b)

Barbaro, Michael and Zeller, Tom Jr. „A Face is Exposed for AOL Searcher No. 4417749." New York Times. August 9, 2006:
http://www.nytimes.com/2006/08/09/technology/09aol.html

Cowan, Rosie. „New crime unit crawls inside killers' minds. Psychologists and police profile past offenders to identify future murderers." The Guardian. Juli 5, 2004:
http://www.guardian.co.uk/uk_news/story/0,3604,1254042,00.html

Hafner, Katie and Richtel, Matt. „Google Resists U.S. Subpoena of Search Data." New York Times. Januar 20, 2006:
http://www.nytimes.com/2006/01/20/technology/20google.html

Karnitschnig, Matthew. „AOL Tech Chief Resigns Over Issue Of Released Data." The Wall Street Journal. August 22, 2006:
http://online.wsj.com/article/SB115618361010241207.html

Meusers, Richard. „Peinliche Pannen bringen StudiVZ in Verruf." Spiegel. November 15, 2006:
http://www.spiegel.de/netzwelt/web/0,1518,448340,00.html

Poulsen, Kevin. „MySpace Predator Caught by Code." Wired News. Oktober, 16, 2006:
http://www.wired.com/news/technology/0,71948-0.html

New York Times. „Stolen Lives: The Problem of Identity Theft." New York Times. 2005-2006:
http://www.nytimes.com/national/nationalspecial2/

Sharkey, Joe. „Laptops give up their secrets to U.S. customs agents." International Herald Tribune. Oktober 24, 2006:
http://www.iht.com/articles/2006/10/24/business/laptop.php

Speck, Hendrik and Thiele, Frédéric Philipp. „Suchmaschinenpolitik. Google is watching you!." 21C3. Dezember 27, 2004

Speck, Hendrik und Thiele, Frédéric Philipp. „Google, Gossip, PR-ostitution. Das Geschäft einer Suchmaschine". in: Lehmann, Kai and Michael Schetsche (Hrsg.). Die Google-Gesellschaft. Transcript. April 2005

Sullivan, Bob. „Bad-news data letters push consumers to stray. Millions dump companies that leaked personal information, study finds." MSNBC. Oktober 4, 2005:
http://www.msnbc.msn.com/id/9581522/

Zeller, Tom Jr. „Link by Link. An Ominous Milestone: 100 Million Data Leaks." New York Times. Dezember 18, 2006:
http://www.nytimes.com/2006/09/25/technology/25link.html (2006a)

Zeller, Tom Jr. „93,754,333 Examples of Data Nonchalance." New York Times. September 25, 2006:
http://www.nytimes.com/2006/09/25/technology/25link.html (2006b)

Selbstdatenschutz

von 46halbe und erdgeist

Nachdem wir nun aus verschiedenen Perspektiven unsere Bedenken ausgeführt haben, die wir gegenüber der um sich greifenden Überwachung haben, könnte beim geneigten Leser schon das schale Gefühl aufkeimen, daß man doch eh nichts tun könne, daß die Spezialexperten aus Staat und Wirtschaft weiter neue Wege finden werden, immer tiefer in uns hineinleuchten zu können, jedem Schritt zu folgen und jeden Gedanken zu protokollieren. Doch wer sind denn hier die eigentlichen Spezialexperten was den Schutz von privaten Daten angeht? Das sind ja wohl wir. Wenn wir keine technischen oder andersartigen Gegenmaßnahmen ergreifen, wer denn dann?

Selbstdatenschutz war schon immer eine Frage des Wissens. Wenn man nicht weiß, wer wo wie wen abschnorchelt, kann man sich nicht schützen. Anhand praktischer Beispiele, die den meisten im täglichen Leben begegnen, wollen wir daher versuchen, auf die Fallstricke der zarten Maid Privatheit hinzuweisen. Da, wo uns das Datenschutzgesetz und der ohnehin vollkommen überbewertete Richtervorbehalt nicht mehr hilft, müssen wir das Heft selber in die Hand nehmen.

Nun – wie kann man sich im Detail vor der allgegenwärtigen Ausspioniererei von staatlicher und privater Seite schützen? Was kann der Bürger im Rahmen der freiheitlich demokratischen Grundordnung tun, um sich und anderen wieder Stück für Stück Privatsphäre zurückzuerobern? Nicht jeder Vorschlag ist perfekt, aber viele sind auch für den täglichen Gebrauch gegen hoheitliche Maßnahmen und andere Schnüffler anwendbar. Denn wenn Daten nicht anfallen, zugeordnet und gesammelt werden können, stellt sich nachher das Problem des Mißbrauchs oder der falschen Verdächtigung gar nicht erst.

Immerhin wissen wir aus den vergangenen Jahren, daß die informationelle Selbstbestimmung nur theoretisch eine prima Sache ist. Praktisch muß man ein Grundrecht auch immer selbst verteidigen, sonst geht es unweigerlich verloren. Außerdem will man nicht der einzige weit und breit sein, der seine E-Mails verschlüsselt oder nicht jubelnd „hurra“ schreit, wenn die eigene Wohngegend mit glotzenden Kameras bestückt wird, oder der sich damit abfindet, als „Anschlußüberlasser“, „Risikoperson“, „Nachrichtenmittler“ oder „Gefährder“ statt als freier Bürger gesehen zu werden. Es reicht ja vollkommen, wenn die anderen Menschen einen schon wegen der Haare oder Klamotten schief ansehen.

Die folgenden Hilfestellungen wurden von vielen Aktivisten aus dem Umfeld des CCC zusammengetragen. Und ihr, liebe Leser, müßt den ganzen Krempel nach dem Lesen nur noch Eurer Mama erklären, zumindest aber Euren nicht-nerdige Freunden. Danach müßt ihr Euch leider auch noch hinsetzen und alltagstaugliche GUIs für ebenjene Mama schreiben, die Ihr hernach als Open Source raushauen könnt. Sport frei!

> Glaub keinem, der dir sagt,
> daß du nichts verändern kannst,
> Die, die das behaupten,
> haben nur vor Veränderung Angst
> Es sind dieselben, die erklären,
> es sei gut so, wie es ist.
> Und wenn du etwas ändern willst,
> dann bist du automatisch Terrorist.
>
> — Die Ärzte, Deine Schuld

Mobiltelefone

Dr. Angela Merkel kam 1990 zur CDU und ging 2005 in die Geschichte ein: als erste Kanzlerin der Bundesrepublik Deutschland.

Da Mobilfunknummern inzwischen nicht mehr ohne weiteres – also ohne Vorlage des Personalausweises – vergeben werden, ist das anonyme mobile Telefonieren recht schwierig geworden. Wer erreichbar sein, nicht ständig Leute um ihr Telefon anschnorren oder sich nicht in eine Telefonzelle stellen möchte, muß einigen Aufwand betreiben.

Natürlich bestünde die Möglichkeit, mit Hilfe anonymisierter Zahlungswege ein Satellitentelefon zu erwerben und zu betreiben. Dank des Preisverfalls ist das nicht einmal mehr wirklich teuer. In der Realität bleibt „für den Rest von uns“ jedoch nur das normale Handy.

Sollte uns nun aus heiterem Himmel ein tatsächlich anonymes Mobiltelefon in die Hände fallen, muß man diesen Zustand verteidigen. Denn Handys geben fortwährend eine ganze Menge Informationen über ihre Nutzer ab. Wenn man nicht aufpaßt, ist man schnell wieder identifiziert. Zwei besonders wichtige Punkte dabei sind IMEI-Nummern und das Problem der Lokalisierung.

Die IMEI und die IMSI

Wenige Handy-Benutzer sind sich der Folgen der Existenz einer eindeutigen Gerätekennung bewußt. Die eindeutige IMEI-Nummer (International Mobile Equipment Identity) eines Telefons wird bei dessen Nutzung mitübertragen und bei den Mobilfunkanbietern systematisch gespeichert und soweit möglich mit den Bestandsdaten assoziiert. Eine neue SIM-Karte, die in ein bereits dort gespeichertes Telefon gesteckt wird, kann also mit den bekannten Benutzerdaten verknüpft werden und ist damit deanonymisiert. Die Informationen, insbesondere zu Telefonen, die mit einem Vertrag erworben wurden, werden je nach Mobilfunkanbieter auch direkt bei heute routinemäßig durchgeführten Bestandsdatenabfragen an die Behörden weitergegeben. Erhält man also eine anonyme SIM-Karte und steckt diese irgendwann einmal in ein Handy, das vorher auf den eigenen Namen (mit einer nicht-anonymen SIM-Karte) gemeldet war, dann war‘s das wieder mit der Anonymität.

Andersrum funktioniert das übrigens genauso. Hat man ein anonymes Handy ein einziges Mal mit einer nicht-anonymen SIM-Karte benutzt, ist das Handy selbst danach nicht mehr anonym. Ebenfalls wichtig zu wissen ist, daß natürlich auch alle Nummern, die man nicht-anonym je gewählt hat und die einen selbst je angerufen haben, gespeichert und profiliert sind, selbst wenn man nicht offiziell unter Überwachung steht.

Durch das Kombinieren von Nutzungsdaten können also Rückschlüsse auf den Benutzer gezogen werden. Hier hilft nur häufiger Wechsel der anonymen Handys und SIM-Karten. Falls man mehrere Handys nutzt, sollte man strikt vermeiden, die einzelnen sozialen Gruppen, mit denen man interagiert, mit jedem der Handys anzurufen. Dadurch wird das Profiling, ermittelt über die Anrufer und Angerufenen und die Häufigkeit dieser Verbindungen, erschwert.

Lokalisierung

Mobiltelefone nehmen naturgemäß Kontakt zu allen nahegelegenen Mobilfunkzellen auf. Beim Einbuchen geben sie dort ihre IMEI bekannt. Somit trägt jeder Benutzer einen personalisierten Peilsender mit sich herum. Wer über die entsprechende Empfangstechnik verfügt (gemeinhin die Telekom-Unternehmen und der Staat), kann in der Folge jederzeit und laufend jeden Handybesitzer auf einige hundert bis wenige Meter genau orten. Die Polizei nutzt diese Möglichkeit seit langem, um die täglichen Aktivitäten von mehr oder weniger Verdächtigen lückenlos und ohne jeden Personalaufwand zu überwachen, zu speichern und zu profilieren.

Und natürlich können anonymisierte Mobiltelefone damit auch wieder Nutzern zugeordnet werden, sei es schlicht durch die Heimatadresse oder durch ein bestimmtes Bewegungsprofil. Vor dieser fortwährenden Lokalisierung kann man sich eigentlich nur schützen, indem man das Handy abschaltet. Auf der sicheren Seite ist man, wenn man im Falle sicherheitskritischer Gespräche frühzeitig einfach den Akku herausnimmt.

Eine hinreichende Anonymisierung für eine begrenzte Zeit ist also nur zu erzielen, wenn SIM-Karten und Telefone zum Einsatz kommen, die nicht zuvor in irgendeinem Zusammenhang mit dem Benutzer standen. Ein einzelner Fehler, etwa ein Telefonat mit einer zuzuordnenden Nummer, kann die Anonymität kompromittieren. Im Alltag ist diese Art Disziplin erfahrungsgemäß nur schwierig aufrechtzuerhalten, und selbst bei Einhaltung aller Regeln sind auf längere Sicht Nutzer durch Analyse der Kommunikationsmuster identifizierbar.

Keylogger und Keyloggerinnen

Das meistgenutzte Eingabegerät heutiger Computer ist zweifelsfrei die Tastatur. Viele relevante Daten, wie z. B. Paßworte, PINs und TANs, aber auch URLs oder E-Mails, werden mit ihrer Hilfe digitalisiert und für die Weiterverarbeitung gespeichert oder versendet. Für alle diese Daten finden sich potentielle Lauscher, seien es kriminelle Kontoleerräumer oder der Staat.

Falls es jemand darauf abgesehen hat, an private Daten zu kommen, ist eine der geeigneten Maßnahmen des Angreifers die Installation eines den uneingeschränkten Zugriff auf die Tastatureingaben bietenden Keyloggers – manche sind leicht detektierbar, andere fast unauffindbar. Nicht erst seit dem berühmten Fall des Mafioso Nicodemo Scarfo, an dessen Bürocomputer das FBI 1999 einen Keylogger installierte, sind derartige Wanzen verbreitet. Der gute Scarfo hatte nämlich Teile seiner Platte mit PGP gegen eine heimliche Durchsuchung gesichert, aber der nicht entdeckte Keylogger brachte dem FBI dennoch den gewünschten Erfolg. [3]

Der Sinn eines Keyloggers wird schon vom Namen angegeben: Der Tastendruck-Protokollierer zeichnet alle Zeichen, die man über die Tastatur eingibt, auf. Diese Informationen sendet er an den "Bedarfsträger" oder Privatschnüffler. Es kann durchaus auch mal eine E-Mail sein. So erhält der Angreifer beispielsweise den Key für das Kryptovolume, den E-Mail-Account oder den SSH-Chat, ohne daß er sich physischen Zugriff auf den Rechner verschaffen muß. Auch Zugangsdaten für externe Speicher im Netz können so erlangt werden, denn BKA-Chef Ziercke hat ja der taz im März erklärt, daß die bösen Terroristen ihre „Daten oft sogar ganz in die Weiten des World Wide Web ausgelagert" hätten, sodaß die Polizei „den Schlüssel zu diesem Versteck" finden will.

Da uns ja die Computerwanze (leicht euphemistisch auch "Online-Durchsuchung" genannt) demnächst ins Haus steht, ist etwas Wissen über Keylogger sicher zukunftsweisend. Man unterscheidet zwei Arten: Zunächst gibt es Keylogger als Hardware. Sie zeichnen Tastatureingaben auf. Das sind kleine Geräte, die man auf der einen Seite in die Tastatur-Steckdose des Rechners steckt, und die andere Seite dann mit dem Tastaturkabel verbindet. Hardwarekeylogger (Bild) müssen also auf physikalischem Weg in die Verbindung von der Tastatur zum Rechner eingebracht werden. Dabei muß die Hardware natürlich nicht unbedingt offen sichtbar zwischen dem Keyboard und dem Computer hängen, es gibt eine breite Auswahl an internen Keyloggern. Wenn man also seiner physikalischen Umgebung nicht trauen kann, lohnt es sich stets, ein eigenes Keyboard dabeizuhaben.

Geht es um den Rechner zuhause – falls man vermuten muß, daß dieser kompromittiert wurde, weil man vergessen hat, die Tastatur mit Epoxyharz zu versiegeln – hilft es, sich schlicht eine neue Tastatur zuzulegen. Die weitere Keyloggerlosigkeit läßt sich mit einem beliebigen "tamper evident"-Mechanismus belegen. Ab und an das Innenleben des Computers nach merkwürdigen elektronischen Komponenten zu untersuchen, hat natürlich noch niemals geschadet.

Ebenso schwierig ist der Schutz gegen elektromagnetische Abstrahlung der Tastaturen bzw. der Kabel. Hier hilft nur die totale Abschirmung. Bei Kabeln reicht es dabei schon, sie einmal in Aluminumfolie einzuwickeln, Tastaturen und Rechner hingegen sind sehr schwer komplett abzuschirmen. Für besonders gefährdete Personen gibt es Kupfertapete und metallbedampfte Scheiben. [1]

Freiwillig strahlen Funktastaturen aller Art – ob per Infrarot, Funk oder Bluetooth. Trotz teilweise integrierter Verschlüsselung der Funkübertragung sollte auf ihren Einsatz am besten verzichtet werden.

Ist der Keylogger Software, kann es etwa der Bundestrojaner oder ein beliebiges anderes Trojanisches Pferd sein. Zumindest beim Bundestrojaner wissen wir ja seit den aus Versehen veröffentlichten Antworten des Bundesinnenministeriums auf den Fragenkatalog der SPD, daß dieser vorzugsweise E-Mails befreundeter Behörden verwendet. Also immer schön aufpassen, wenn der nette Sachbearbeiter im Bauamt, der eigentlich gar nicht so aussieht, als könne er überhaupt einen Browser bedienen, plötzlich E-Mails schickt und um Ausfüllen des angehängten Formulars bittet. Sollte es sich um einen ernsthaften Angreifer handeln, sind heute bereits ausgesprochen ausgefeilte Spionageprogramme bekannt, denn die Grenzlinie zwischen Keyloggern und Rootkits verläuft zuweilen fließend.

Der zweite, deutlich unauffälliger zu installierender Typ von Keyloggern sind also Softwarelogger. Sie hängen sich zwischen den Gerätetreiber der Tastatur und das Betriebssystem. [2] Durch zusätzliche Programme läßt sich außerdem ihre Existenz in Überwachungstools verstecken. Da in der Regel administrativer Zugriff zur Installation der Sniffer nötig ist, sollte das System immer auf dem neuesten Stand gehalten werden, sprich Updates regelmäßig eingespielt werden. Aber Vorsicht, auch in solchen Updates lassen sich Schadprogramme wie Keylogger unterbringen. Den einzigen Schutz bietet eigentlich nur, den Rechner komplett vom Netzwerk zu trennen. Im Zweifel nutzt aber auch das nichts. Wie den Aktivitäten des Verfassungsschutzes im Rahmen der sog. Online-Durchsuchung zu entnehmen ist, können auch klassische Verfahren, wie das heimliche Eindringen in die Wohnung, mit der Installation von Keyloggern kombiniert werden. Die einzige Maßnahme gegen solche Eingriffe bieten sichere Entsperrpaßworte auch schon beim Anschalten des Rechners.

[1] *http://www.heimwerker.de/heimwerker/heimwerker-beratung/wandgestaltung-und-dekoration/tapete-und-tapeten-sorten/tapeten-tapetenarten/abschirm-tapete-emv-tapete.html*
[2] USBmon *http://www.hhdsoftware.com/Products/home/usb-monitor.html*
[3] United States vs. Scarfo, *http://www.epic.org/crypto/scarfo.html*

Die Hardware-MAC-Adresse

Jede Netzwerkkarte, egal ob kabelgebundenes Ethernet oder drahtloses WLAN, hat eine weltweit eindeutige 48 Bit lange Identifikationsnummer, die MAC-Adresse. Diese Hardwareadresse ist meist in einem EEPROM auf der Karte gespeichert und dient zur niederschichtigsten Adressierung eines Computers in einem Netzwerk. Sobald man sich also mit einem Netzwerk verbindet, ist man automatisch anhand der MAC-Adresse identifizierbar, zumindest innerhalb dieses Netzwerkes.

Um dies zu umgehen, besteht die Möglichkeit, seine MAC-Adresse zu ändern. Tut man dies regelmäßig, ist eine Zuordnung des eigenen Computern deutlich erschwert. Unter dem Betriebssystem Linux ist beispielsweise das Ändern der MAC-Adresse mit nur einem Kommandozeilenbefehl möglich.

```
ifconfig <iface> hw ether <MAC-Adresse>
```

Dabei muß die MAC-Adresse aus hexadezimalen Ziffern in der Form xx:xx:xx:xx:xx:xx aufgebaut sein. Unter FreeBSD und MacOSX läßt man den Parameter “hw” einfach weg. Unter Windows kann die Hardwareadresse in der Registry geändert werden. Eine genauere Beschreibung gibt es hier [1], ein Programm unter [2]. Ändert man die eigene MAC-Adresse, gehen natürlich alle offenen Verbindungen verloren.

[1] http://www.nthelp.com/NT6/change_mac_w2k.htm
[2] http://ntsecurity.nu/toolbox/etherchange/

Die IP-Adresse

Natürlich ist auch die IP-Adresse ein relativ eindeutiger Identifier, und das auch noch weltweit. Zwar kann man den normalen Heiminternetnutzer nicht direkt erkennen, aber man bekommt zumindest den Provider raus, und der gibt leider all zu leichtfertig seine Kundendaten preis. Nach dem Gesetz zur Reform der Telekommunikationsüberwachung sind diese Verbindungsdaten sechs Monate zu speichern.

Wie verhindert man also, daß die Betreiber von Webseiten oder die Besitzer von Rechnern auf dem Weg des Paketes an die IP-Adresse des eigenen Rechners kommen? Eine Möglichkeit ist die Verwendung von sogenannten Proxyservern. Proxies dienen als Zwischenschritt der Webanfrage. Anonyme Proxies ersetzen dabei die IP des Absenders durch ihre eigene. Für alle nachfolgenden Hops auf dem Weg zum Ziel erscheint somit der Proxyserver als Ausgangspunkt der Anfrage.

Oft werden aber auch noch andere Informationen über den Browser bzw. das Betriebssystem in einer Anfrage mitgeliefert, die ebenfalls zur Identifizierung eines Rechners herangezogen werden können. Überprüfen kann man die übermittelten Daten, inklusive der IP-Adresse, beispielsweise unter *http://kluge.in-chemnitz.de/tools/browser.php* und somit feststellen, inwieweit ein Proxyserver zufriedenstellend funktioniert.

Proxyserver leiten in der Regel die Anfragen nur weiter, ohne deren Inhalt zu verschlüsseln. Somit ist weiterhin jeder Mitnutzer des eigenen Netzwerkes sowie der Provider in der Lage, Informationen über den Content der besuchten Webseiten einzusehen. Eine Alternative hierzu bietet der verschlüsselte Proxydienst TOR.

Wenn Cookies rumkrümeln

Besonders notorisch gefährliche Internet-Abhörer sind Cookies. Cookies werden meist automatisch von bestimmten Webseiten auf den Computern der Nutzer installiert und beinhalten für die Seite relevante Informationen über die Nutzer, die dann bei jedem neuen Aufruf der Seite sofort abgerufen werden können. Damit können sie allerdings auch mißbraucht werden. Etwa indem andere Seiten die gespeicherten Infos abfragen oder ungefragt eigene Cookies installieren, können Fremde Auskünfte über das Verhalten der Nutzer im Internet erhalten, die illegitim weitergenutzt werden können, etwa zum "Profiling" durch Data-Mining.

Man sollte daher öfter mal in den Einstellungen des Browsers nachsehen, wer da alles Cookies installiert hat und die unbekannten oder unerwünschten löschen und für die Zukunft blokkieren. Das ist gefahrlos, denn Seiten, die man selbst braucht und die ohne Cookies nicht funktionieren wollen, kann man ganz einfach in den Einstellungen des Browsers wieder entblockieren.

Wichtig ist auch zu wissen, daß sogar die Nutzung von Proxies wie TOR nicht unbedingt vor Cookies schützen. Selbst mit Benutzung der Proxies kann immer noch jeder feststellen, wo wer wann war, wenn er eben Zugang zu den Cookie-Dateien auf dem Computer hat. Wichtig ist deshalb auch für TOR-Nutzer, in den Einstellungen des Browsers regelmäßig die Cookies zu überprüfen und die, denen man nicht traut, zu löschen.

Noch gefährlicher wird es, wenn man TOR ab und zu ausschaltet. Kommt man dann auf Seiten, die eine individuelle ID für ihre Nutzer haben und vielleicht irgendwo ein kleines Werbebanner mit JavaScript und einem Cookie drin, kann der TOR-Traffic leicht mit dem Nicht-TOR-Traffic korreliert werden (*doubleclick.net* macht das zum Beispiel). Für solche Seiten stellt man am besten in den Einstellungen ein, daß man nur Cookies von Originalseiten erlaubt – dann können weniger Fremdabfragen kommen.

Cookies lassen sich außerdem auch gut mit Firefox-Erweiterungen handhaben. Cookie Culler und CookieButton zum Beispiel installieren Toolbars, über die man laufend unerwünschte Cookies löschen und blockieren kann. Add'N'Edit Cookies erlaubt einem, Cookies auf Seiten zu lokalisieren, sie zu modifzieren, zu löschen oder wieder hinzuzufügen. Da Cookies sich außerdem auch in Google-Anfragen, anderen JavaScript-Anwendungen und in der Linkauswahl befinden können, sollten diese Bereiche auch regelmäßig gereinigt ("gescrubt") werden. Das geht etwa mit scroogle.

Geschichten aus dem Browser

Der Nutzer des Internet gibt auch immer eine große Menge von Informationen über sich preis. Über das Internetverhalten kann man genau nachvollziehen, wer was wann wo macht, und Profiler-Programme können letztendlich auch ein „Warum" daraus schließen – Mißbrauchsmöglichkeiten inbegriffen.

Auf der Benutzerseite speichert der Browser den Verlauf der letzten Internet-Sessions. Diese regelmäßig zu löschen, kann dem Anwender einige Erklärungen ersparen. Dies macht auch Sinn, da JavaScript-Programme im Fenster begrenzt auf diese History zugreifen können. Die regelmäßige Reinigung kann man in den Einstellungen des Browsers („Preferences") einstellen. Daneben tragen auch Werkzeuge wie die Firefox-Erweiterung „NoScript" mit einem Satz weiterer nützlicher Features zum Schutz der Privatsphäre des Benutzers bei.

RFID – Schnüffelchipalarm

Als RFID (Radio Frequency IDentification) werden Systeme bezeichnet, die zur Identifizierung Funk benutzen. Dabei bestehen solche Systeme immer aus einem kombinierten Sende- und Empfangsgerät und dem ID-Tag. Die Tags bestehen aus kleinen Chips und einer auf den Frequenzbereich abgestimmten Antenne.

Passive Tag beziehen ihre gesamte Energie aus dem elektrischen oder magnetischen Feld des Lesegerätes, sind also außerhalb der Reichweite des Feldes nicht in der Lage, ihre Daten zu senden. Aktive Tags haben zusätzlich noch eine eigene Batterie, die ein dauerhaftes Senden auch über größere Distanzen ermöglicht. Will man verhindern, daß ein RFID-System Daten über die anwesenden Tags erhält, gibt es drei potentielle Angriffspunkte: das Sende- und Empfangsmodul, den RFID-Tag und die Kommunikation dazwischen.

Da sich das Sendegerät meist außerhalb des Einflußbereiches befindet, klammern wir es aus der aktuellen Betrachtung einmal aus. Wie schon erwähnt, besteht ein RFID-Tag aus dem Identifikationschip und der daran angeschlossenen Antenne. Trennt man beide voneinander, verringert sich die Reichweite des Systems dramatisch. Gleiches gilt, wenn die Antenne an einer beliebigen Stelle durchtrennt wird.

Eine andere Möglichkeit, die Reichweite zu reduzieren, ist die Verminderung der Feldstärke des elektromagnetischen Feldes und damit der Versorgungsspannung des passiven Chips. Mit dem gleichen Verfahren wird auch die Sendereichweite der aktiven Tags minimiert. Technisch ist das alles andere als schwierig. Schon das Einbringen einer Lage Aluminiumfolie zwischen Leser und dem Tag verhindert zuverlässig die Kommunikation. Dabei muß die Folie mindestens die Größe der Antenne des Tags aufweisen. Eine Hülle aus Metallfolie schützt also effektiv vor dem Auslesen der so verpackten RFID-Karten.

Sowohl bei der Zerstörung der Antenne als auch beim Einwickeln in Aluminiumfolie bleibt der Chip jedoch funktionsfähig und kann zu einem späteren Zeitpunkt wieder ausgelesen werden. Will man dies endgültig verhindern, bleibt nur die Zerstörung des Chips. Eine sehr einfache und wirkungsvolle Methode ist das Verursachen mechanischer Belastung. Gezielte Hammerschläge auf die Stelle, an der sich der Chip befindet, führen früher oder später zum Erfolg. Optimieren läßt sich das Ganze durch die Verwendung dünner, aber stabiler Nadeln, die, auf den Chip gesetzt, die Kraft der Hammerschläge gebündelt auftreffen lassen.

Dazu ist allerdings die Positionsbestimmung des Chips in der RFID-Karte nötig. Hierbei kann eine helle Lichtquelle hilfreich sein. Hält man den Randbereich der Karte gegen das Licht, sieht man dünne parallel verlaufende Schatten: die Antenne. Meist an einer der Ecken ist diese mit einem nur wenige Millimeter großen Quadrat verbunden.

Neben mechanischen Kräften können aber auch elektromagnetische Pulse hoher Energiedichte einem RFID-Tag den Garaus machen. Klingt wie Alientechnologie? Ist es aber nicht. Nahezu jeder hat inzwischen eine EMP-Gun bei sich in der Küche zu stehen: eine Mikrowelle. Um Muttis leckeres Essen vom Vortag aufzuwärmen, sendet diese elektromagnetische Wellen von mehreren 100 Watt auf einer Frequenz von 2,4 Gigahertz aus. Treffen diese auf den hilflosen RFID-Chip, bleibt dem in der Regel nichts anderes übrig, als innerhalb von kürzester Zeit zu explodieren. Diese nachhaltige Zerstörung ist zwar meist ungefährlich, aber nicht immer unsichtbar, wie unser Versuch an einem WM-Ticket erbracht.

Da die mutwillige Zerstörung des Chips am besten unentdeckt bleiben sollte (ja, der ePass mit integriertem RFID-Chip ist auch mit defektem Chip weiterhin gültig) und man auch nicht unbedingt eine Mikrowelle zu jedem Einkaufs-

bummel mit sich rumschleppen will, gibt es die EMP-Gun jetzt auch in handlich und zum selberbauen. Dazu benötigt man lediglich einen Wegwerffotoapparat und einen Lötkolben. Nach dem vorsichtigen Öffnen des Apparates entfernt man das Blitzlicht und lötet an dessen Stelle einen Draht an.

Optimalerweise wird dieser in drei bis vier Schlaufen auf die Größe der Antenne des Opfer-RFID-Chips gebracht. Statt nun einen optischen Puls in Form eines Blitzlichtes auszulösen, sendet der „RFID-Zapper“ einen elektromagnetischen Puls durch die Antenne und auf den RFID-Chip. Die Reichweite ist dabei sehr begrenzt (wenige Zentimeter), man sollte den Zapper zur Sicherheit aber nur in größerer Entfernung (ein Meter ist ausreichend) zu lebensnotwendiger Hardware wie Computern oder Herzschrittmachern einsetzen.

Die Zerstörung ist irreversibel. Die Mutwilligkeit ist nur mit sehr, sehr großem Aufwand nachweisbar – wenn überhaupt. Um sich nicht komplett in Alufolie einwickeln zu müssen oder jedes Kleidungsstück bis hin zur Unterhose in die Mikrowelle zu stecken, gibt es auch noch andere Möglichkeiten, vorhandene RFID-Tags vor dem unberechtigten Auslesen zu schützen. Dazu kann man die Kommunikation der Chips mit dem Lesegerät entweder vollständig oder nur diffizil das Übertragungsprotokoll stören.

Eine Komplettstörung kann relativ einfach durch einen Sender erreicht werden, der auf der gleichen Frequenz wie die RFID-Chips arbeitet und eine höhere Sendeleistung besitzt. Durch das Aussenden von Rauschen kann jegliche Kommunikation effektiv gestört werden. Da die Übertragung vom Chip zum Lesegerät meist auf einer Nebenfrequenz bei deutlich geringerer Leistung abläuft, ist es sinnvoller, den Störsender hier zu betreiben. Für den Betrieb knapp über der Rauschschwelle reichen Batterien als Spannungsversorgung auch für einen längerfristigen Betrieb in der Nähe von festinstallierten Lesegeräten aus. :}

Noch weniger Strom verbrauchen Sender, die gezielt die Kommunikation oder den Kommunikationsaufbau auf Protokollebene stören. Um mehrere RFID-Chips im Bereich des gleichen Lesegerätes unterscheiden zu können, haben die meisten Chips eine eindeutige nicht-veränderliche Identifikationsnummer: die UID. Diese ist Ansatzpunkt der Antikollisionsalgorithmen. Durch gezieltes Senden der „richtigen“ UID kann ein Störsender den Kommunikationsaufbau stark verzögern oder vollständig unterbinden.

Die Königsdisziplin ist allerdings das gezielte Ändern einzelner Bits auf dem Übertragungsweg von einem berechtigten Chip zum Lesegerät. Falsche Daten können oft mehr Schaden anrichten und sind außerdem schwieriger zu identifizieren.

All diese Manipulationen sind kaum zu verhindern, weil sie in integrale Teile des Systems eingreifen und mögliche Schutzmechanismen, wie beispielsweise das Signieren der Daten, aufgrund der geringen Rechenleistung der aktuellen RFID-Chips schwer zu implementieren sind.

Anonymes Publizieren im Netz

Um Informationen im Internet zu veröffentlichen, während man Interesse daran hat, nicht als deren Urheber identifiziert werden zu können, bieten sich verschiedene Wege an. Einerseits kann man, die üblichen Vorsichtsregeln beachtend, Web-Foren und öffentlich archivierte Mailinglisten benutzen. Wer aber andererseits sicher sein möchte, daß diese Inhalte auch veröffentlicht bleiben, muß sich schon selber um sein Serverplätzchen kümmern.

Schon das Reservieren einer Domain geht im Allgemeinen mit der Preisgabe seines Namens einher. Allerdings gibt es Provider, die Domains anonym hosten. Diese akzeptieren beispielweise Geld von einem e-Gold-Offshore-Konto als Bezahlung. Alternativ kann man zur Zahlung auch eine Kombination anonymer Methoden wie Money Orders, anonyme Kreditkarten oder Pre-Paid Debit Cards wählen, um eine Domain bei einem der "normalen" Provider hosten zu lassen. Registrare für kleinere Top-Level-Domains wollen üblicherweise nur irgendeine belastbare Kreditkartennummer sehen.

Verbreitet man auf der Webseite Wissen, das potentiell Ärger mit den Ermittlungsbehörden oder den überbezahlten Anwaltsscharen privater Unternehmen nach sich ziehen könnte, empfiehlt es sich, die Domain im befreundeten Ausland hosten zu lassen. Der frühere europäische Ostblock bietet da viele Möglichkeiten, wo preiswertes Unix-Hosting inklusive Domain-Registrierung feilgeboten wird.

Auch wenn man der festen Überzeugung ist, daß alle Inhalte der Webseiten vom Grundrecht auf Rede- und Meinungsfreiheit gedeckt seien, ist man so auf der sicheren Seite. Ein Prozeß vor dem Bundesverfassungsgericht ist bekanntermaßen eine langwierige Sache.

Eine einfache Google-Suche nach "offshore hosting" liefert zahlreiche Treffer, die Nummer eins ist derzeit der in den Hongkong ansässige WRZHost. Da lohnt es sich also, mal die zweite Ergebnisseite aufzurufen. Zudem sollte man sich vorher mit der Preisstruktur vertraut machen, meistens bezahlt man sehr viel für den Traffic.

Wenn man darauf angewiesen ist, gesetzlicher oder andersgearteter Zensur zu entgehen, sollte man darauf achten, daß der gewählte Hosting-Provider tatsächlich im nicht allzu befreundeten Ausland angesiedelt ist. Ein simples `whois` hilft da schon weiter. Nicht, daß man am Ende nur bei einer Tochter deutscher oder gar US-amerikanischer Firmen landet, die bei der ersten angeblichen Rechtsverletzung artig und DMCA-konform die Webseite geordnet herunterfährt.

Möchte man eine verschleiernde Schutzschicht drauflegen, bietet sich als weitere Option an, einen Account bei einem OpenVPN-Provider zu verwenden. Damit kann man dann seine Domain an der geographischen Örtlichkeit seiner Wahl hosten, unabhängig von der Server-IP-Adresse.

Dabei muß beachtet werden, daß jeder, der ein Traffic Monitoring am Server durchführen kann, in der Lage ist, die Ursprungs-IP-Adresse herauszufinden. Daher ist der Tunnel zum OpenVPN-Provider nur in Verbindung mit anonymem Hosting empfehlenswert, wenn man ernsthaft unidentifizierbar sein will oder muß. Was man also damit tatsächlich erkauft, ist ein kleines bißchen Vorwarnzeit, wenn nämlich der VPN-Service zuerst runterfährt.

Hat man den OpenVPN-Account bereits am Start, kann man sich zu dem OpenVPN-Provider auch mittels TOR oder eines http-Proxy verbinden. Hat man nämlich die Verbindung zum VPN hinbekommen, ist es kaum schwieriger, sich zum TOR-Netzwerk zu verbinden. Allerdings sollte hier beachtet werden, daß die Verbindung über TOR weniger stabil und schnell sein wird.

Reflexionen über Kameras

Um Überwachungskameras auszuschalten oder um Aufmerksamkeit auf diese zu ziehen, gibt es viele Wege.

Eine erste Möglichkeit besteht darin, normale Wandfarbe zu gleichen Teilen mit Wasser zu mischen: Abgefüllt in einem Supersoaker läßt sich dieses Gemisch aus vier bis fünf Metern Entfernung gezielt versprühen. Dabei sollte man zunächst seine Aufmerksamkeit auf die Linse richten, hinterher aber auch noch den Kamerakörper abdecken (damit kann man häufig auch andere empfindliche Teile verschmutzen).

Einen weniger dichten Farbauftrag kann man mit Paintballpistolen erzielen, dafür hat man mit diesen Pistolen aber eine deutlich größere Reichweite. Die Farbkügelchen, die bei dieser Freizeitbeschäftigung normalerweise die Spieler der gegnerischen Mannschaft markieren, eignen sich prima zum Verschmaddern einer Linse. Besonders herausragend scheint hier die Farbe, die in Fachkreisen als „Taubenkakke“ bekannt ist. Geübte Aktivisten können mit den Pistolen noch auf 50 Meter eine schmucke Dekoration applizieren, nostalgischen Gemütern sei hier eine Zwille nahegelegt. Mit dieser sollen – Gerüchten zufolge – immer noch 25 Meter Zielentfernung zu schaffen sein, wenn die Bälle auf der Kamera zerplatzen und nicht schon in der Hand.

Auch ein davorgeklemmter Spiegel liefert den Überwachern kurzfristigen Spaß für den Nachmittag. Schöne Ergebnisse liefern lustigerweise auch Klarlack und Haarspray. Diese Substanzen sorgen nicht durch mangelnde Transparenz für fehlenden Durchblick – sie verhunzen durch den unebenen Auftrag den Lichtbrechungseffekt der Linse.

Eine ineffiziente Methode sind Laserpointer: Ab fünf Milliwatt sind diese prinzipiell bei etwas längerer Einstrahlung in der Lage, Kameras kurzfristig erblinden zu lassen oder auch langfristig zu schädigen. Allerdings muß dazu der Strahl über einige Zeit still gehalten werden – und dabei ist die Gefahr, einen reflektierten Strahl in die Augen zu bekommen, leider nicht von der Hand zu weisen.

Für das temporäre Ausblenden von sich selbst bietet es sich an, die Empfindlichkeit der meisten Kameras im Infrarotbereich auszunutzen. Eine lichtstarke IR-Diode auf den Kopf geschnallt: Schon erzeugt man bei vielen Überwachungssystemen grelle Flecken an genau der Stelle, an welcher sonst das Gesicht gespeichert würde. Dies funktioniert leider nur bei Kameras, die im IR-Band auch wirklich empfindlich sind. Die meisten im Tageslicht arbeitenden Geräte sind jedoch mit einem IR-Filter vor dem entsprechenden Farbanteil im Sonnenlicht geschützt.

Sollten Bilder von der Kamera zu den Überwachern über Funktechnologien übertragen werden, helfen Jammer im entsprechenden Frequenzbereich, meistens 2,4 Gigahertz. Allerdings stört man damit auch die WLANs der Anwohner, was nicht unbedingt zur Freude in der Nachbarschaft beiträgt.

Ebenfalls zerstörungsfrei – aber sozialer – kann man sein Recht auf die informationelle Selbstbestimmung schlicht durch Wegdrehen durchsetzen. Natürlich nicht sich selbst, sondern die Kamera. Mit einer Teleskopstange aus dem Malerbedarf kann man dabei auch Kameras, an die man selbst mit Kletterschuhen nicht herankommt, zum idyllischen Sternenhimmelgukken überzeugen.

Weniger elegante, aber durchaus gängige Vorgehensweisen bestehen darin, mit Äxten oder Zangen die Kabel zu durchtrennen oder die Kameras einfach mit Steinen zu zerstören (das geht am besten von oben). Der eine oder andere Nerd soll auch schon dabei beobachtet worden sein, sich zu Forschungszwecken ein solches Gerät einfach abgeschraubt zu haben.

Tracking torrents

„With BitTorrent free speech no longer has a high price." – Bram Cohen

Das von Entwickler Bram Cohen entwickelte P2P-Programm BitTorrent erfreut sich großer Beliebtheit. Im BitTorrent-Protokoll ist vorgesehen, daß sich Datentauschwillige finden, indem sie ihre IP-Adresse bei einem sog. Tracker hinterlegen und gleichzeitig die IP-Adressen anderer Interessenten (Peers) abholen.

Einige wenige BitTorrent-Programme unterstützen mittlerweile das Routing zum Tracker und anderen Peers über das TOR-Netzwerk. Die Datenverbindungen zwischen Peers über TOR ist aber keine wirklich gute Idee, denn die zusätzlichen Datenmengen verlangsamen die Benutzung für alle anderen Benutzer. Rudimentären Schutz bietet hier eine primitive, aber schnelle Crypto-Option, die in einigen BitTorrent-Clients, wie z. B. in Azureus und Transmission, implementiert wurde.

Andererseits macht die Benutzung von TOR für die Kommunikation mit dem Tracker nicht viel Sinn. Schließlich geht es ja darum, gefunden zu werden. Und somit heißt das auch lange nicht, daß die Contentmafia nicht trotzdem an die IP-Adressen kommen könnte, sie braucht den Trakker bloß danach fragen.

Metadaten putzen

Hat man für die anonyme Veröffentlichung von Informationen im Netz alle Vorkehrungen getroffen, muß man aufpassen, sich nicht durch eben diese Informationen zu verraten. Dabei geht es an dieser Stelle nicht um die Auswertung grammatikalischer Strukturen in Bekennerschreiben oder um die Analyse von Kamerablickwinkeln in kompromittierenden Photos.

Viele Dateien tragen begleitende Beschreibungen mit sich, die über die Umstände von Erzeugung oder Änderung Auskunft geben können. Diese werden auch als Metadaten bezeichnet und finden sich in den meisten Dateisystemen als extern gespeichertes Attribut wieder, so zum Beispiel das Datum der letzten Änderung. Für einige Dateitypen ist jedoch vorgesehen, weitaus komplexere Metadaten im Inneren vorzuhalten.

Das populäre Bildformat JPEG – heutzutage von fast allen digitalen Kameras erzeugt – erlaubt Applikationen, beliebige binäre Blöcke mit in der Bilddatei zu speichern. Digitalkameras nutzen den „APP1"-Bereich dazu, Einzelheiten über die Herkunft eines Photos – wie z. B. Hersteller, Typenbezeichner und Seriennummer der Kamera – in sog. Exif-Tags zu kodieren. Die Details Datum, Uhrzeit und GPS-Position der Aufnahme lassen sogar noch genauere Rückschlüsse auf den Photographen zu.

Um diese Informationen sicher aus dem Bild zu entfernen, sollte man es kurzfristig in ein Format konvertieren, in dem es keine Möglichkeit zur Speicherung von Metadaten gibt. Unter Windows bietet sich hier das BMP-Format an. Benutzer von Gimp können das Bild im PPM-Format speichern und sich danach in einem Texteditor davon überzeugen, daß nur rohe RGB-Werte für jeden Pixel, nichts jedoch über den Bildursprung wiedergefunden werden kann.

Vorm Veröffentlichen im Netz sollte das Bild natürlich wieder in eins der klassischen Web-Formate PNG, JPEG oder GIF konvertiert werden. Bei der Wahl des Werkzeugs dafür sollte man jedoch darauf achten, daß dieses nicht wieder Metadaten – wie zum Beispiel die Seriennummer oder den Rechnernamen – einfügt.

Auch bestimmte Textdokumente enthalten viele zusätzliche Daten. Microsofts Textverarbeitung „Word“ erzeugt Dokumente, in denen von Haus aus die Namen der letzten Bearbeiter, der Käufer der benutzten Software und der Zeitpunkt des letzten Ausdrucks gespeichert sind. Bei vielen Benutzern ist es aus Zeitgründen inzwischen üblich, seine Änderungen mittels „Schnellspeichern“ zu sichern. In einem Word-Dokument bis zur Version 2007 sind die Daten binär und wie auf einer Diskette in Blöcken strukturiert. Beim schnellen Sichern werden nur Blöcke mit den Änderungen angehangen, die alte Version ist dabei schon für mittelmäßig begabte Hacker wiederherstellbar.

Ähnliche Probleme mit der Änderungsgeschichte hat das Dokumentenformat PDF. Aus Effizienzgründen werden auch hier bei Änderungen die alten Objekte – wie zum Beispiel Textzeilen oder eingebettete Bilder – nur als freigegeben markiert und ein Objekt mit der neuen Version angehangen.

Statt also Pamphlete als Word-Dokument oder PDF ins Netz zu stellen, sollte man überlegen, seinen Text in einem leichter zu überprüfenden Format wie RTF oder – falls es auf die Formatierung nicht ankommt – gar als TXT zu speichern. Für die ganz Paranoiden bleibt nur, die Dateien auszudrucken und wieder einzuscannen.

Bleibt noch zu erwähnen, daß auch Audiodateien im MP3-Format Sektionen für Metadaten vorsehen, in denen Titel von Stück und Album und der Name des Interpreten zu finden sind. Von diesen Sektionen können sich beliebig viele im MP3 befinden. Einige MP3-Rip-Programme speichern im Kommentarfeld ihren Namen und die Versionsnummer. Mit viel Phantasie lassen sich hierdurch zumindest einige der Aufnahme des Tondokuments Verdächtigte ausschließen.

Anonbox – sichere Empfängnis

Dem Bedürfnis nach anonymem Konsum von Informationen aus dem Internet stellen sich zuweilen seltsame Interessen der Informationsanbieter entgegen. Will man zum Beispiel den Jahresbericht des Landesamtes für Verfassungsschutz lesen, wird dieser als PDF angeboten.

Der Herausgeber bietet das Dokument allerdings nicht auf seiner Webseite – und damit in der Reichweite von TOR – an, sondern schickt es gern per E-Mail zu. Nicht jeder mag seinen Mail-Account in den Logfiles oder Datenbanken des Landesamtes für Verfassungsschutz wissen – schon gar nicht mit dem Vermerk, er hätte sich für ihren Jahresbericht interessiert.

Ebenso Bestätigungen für Zugänge zu bestimmten Online-Diensten, Antworten auf Fragen an Hilfehotlines – man könnte für jede dieser E-Mails den mühsamen Weg beschreiten, einem der Freemail-Anbieter ein Postfach abzuringen und ihn danach wieder zu löschen.

Den einfacheren Weg bietet der Chaos Computer Club unter *https://anonbox.net/* an. Dort kann sich der um seine Anonymität besorgte Benutzer eine Wegwerf-E-Mailadresse besorgen, die für rund 24 Stunden gültig ist und – bei Einhaltung einiger Spielregeln für Anonymität im Internet – den nicht zuordenbaren Empfang von Nachrichten erlaubt. Aber auch auf Serverseite wird durch eine rigide Vermeidung von Logs die Privatsphäre der Anwender geschützt.

Interview mit Anne R.

Lars Sobiraj

Anne ist die bloggende Lebensgefährtin des vom Bundeskriminalamt (BKA) engmaschig überwachten Berliner Soziologen Andrej H. Wegen Begriffen in seinen Fachpublikationen, in denen er Stadtentwicklungsprozesse beschrieb, wurde Annes Lebensgefährte der Mitgliedschaft in der „militanten gruppe" (mg) verdächtigt. Er befand sich von Ende Juli bis zum 22. August 2007 in Untersuchungshaft. Er und seine Familie werden seit über einem Jahr systematisch vom BKA überwacht.

Inzwischen auf freiem Fuß, geht die Überwachung Andrejs und seines Umfeldes ohne Unterbrechung weiter, obgleich die Mitgliedschaft in der mg wegen nur dürftigster Indizien angenommen wurde. Darüberhinaus stellte der Bundesgerichtshof (BGH) am 28. November 2007 fest, daß es sich bei der militanten gruppe nicht um eine „terroristische Vereinigung" im Sinne des Paragraphen 129a StGB handelt. Am gleichen Tag wurden auch die Haftbefehle gegen die drei anderen mit Andrej festgenommenen Personen außer Vollzug gesetzt. Terroristen oder nicht, am Monitoring Andrejs, seiner Lebensgefährtin Anne und der Kinder durch das BKA hat sich nichts geändert.


Anne R.

Lars Sobiraj: Hallo Anne. Wie erging es dir, euren Kindern und deinem Lebensgefährten in dieser Woche? Ich hoffe, außer den defekten Computern, krisselnden Fernsehern und eurer gestörten Telekommunikation ist in den letzten Monaten nicht mehr zu Bruch gegangen?

Anne: Hallo. Nein, kaputtgegangen ist diese Woche nichts. Die Überwachung hat gerade wieder enorm angezogen, also der spürbare Teil davon – zuletzt ist gestern mein Rechner viermal komplett hängengeblieben, als ich an meinem letzten Blog-Eintrag bastelte. Ganz bizarr auch am Dienstag: Da haben wir in der Berliner NGBK eine Veranstaltung gemacht, bei der u. a. der Film „Strange Culture" in Ausschnitten gezeigt wurde, ein Film über ein Verfahren gegen den amerikanischen Künstler Steve Kurtz, gegen den wegen völlig harmloser Bakterien und Reagenzgläser ein Bioterrorismus-Verfahren eröffnet wurde, das heute noch läuft. Die Parallelen werden in dem Film sehr deutlich. Ich habe in der Veranstaltung auch erzählt, wie es sich anfühlt, überwacht zu werden, zu wissen, daß die Überwacher immer da sind, und sah dabei einem indifferent guckenden älteren Herrn ins Gesicht, Strickpulli, deutlich aus dem sonstigen Publikum rausstechend. Das ist schon ziemlich eigenartig. Ansonsten war die Woche so stressig wie alle seit dem 31. Juli, und vor allem aber auch sehr großartig, weil die letzten drei in diesem 129a-Verfahren wegen Terrorismus Angeklagten gegen Auflagen aus der Untersuchungshaft entlassen wurden. Der Bundesgerichtshof hat entschieden, daß alle sieben nunmehr keine Terroristen mehr sein sollen. Sondern „nur noch" kriminell. Das ist, was das Verfahren angeht, nicht wirklich viel besser, allerdings ist das zu erwartende Strafmaß

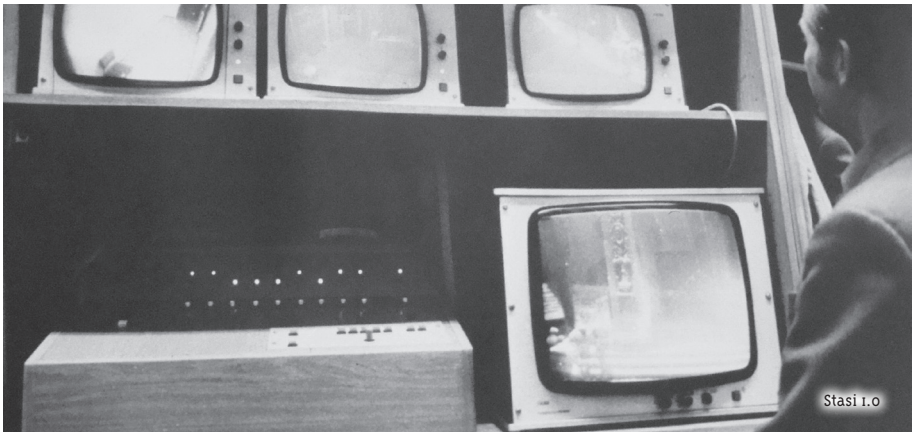
deutlich geringer. Da sind drei Leute fast vier Monate in Untersuchungshaft gewesen, weil sie drei Bundeswehr-LKW angezündet haben sollen und weil einer von ihnen zweimal Andrej getroffen haben soll. Die LKW gibt es immer noch, niemand wurde gefährdet – normalerweise führt das nicht zu Untersuchungshaft. Wir – also alle, die direkt mit diesem Verfahren zu tun haben: Familien, die Beschuldigten selbst, Freundinnen, Mitbewohnerinnen – haben zwar immer gefunden, daß sie freigelassen werden müssen, aber das wirklich zu hoffen, haben wir uns mehrheitlich wohl nicht so wirklich getraut – ein Terrorismusverfahren ist eben doch was anderes als Falschparken.

Ich war am Anfang fassungslos darüber, daß es dieses Verfahren so gibt – bin ich eigentlich immer noch. Zu sehen, daß es möglich ist zu verhindern, daß Leute mit diesem ganzen frei erfundenden Quatsch tatsächlich öffentlich zu Deutschlands Top-Terroristen gemacht werden und das dann auch bleiben, fühlt sich gut an. Auch wenn wir noch einiges vor uns haben.

Nebenbei ist das alles wahnsinnig anstrengend, ich bin jetzt am Ende der Woche vor allem müde. Der ganze Wirbel permanent, dazu zwei Kleinkinder und noch ein bißchen sonstiges Leben, das macht urlaubsreif.

Lars Sobiraj: Die Einträge in deinem Weblog haben offensichtlich viele Menschen sehr nachdenklich gestimmt. Einige der Verdachtsmomente, die als Grund für eure Überwachung angegeben wurden, würden auf unglaublich viele Personen in Deutschland zutreffen. Außer euch beiden leben noch Millionen andere Menschen in diesem Land, die sowohl gebildet, unauffällig, auf ihre Privatsphäre bedacht und irgendwie links eingestellt sind. Was meinst du, sollten die jetzt alle beim Bloggen vermehrt auf das Vermeiden bestimmter soziologischer Fachbegriffe achten? Oder artet das in Paranoia aus?

Anne: Sehr schöne rhetorische Frage. (lacht) Ich glaube, daß gab es seit Echelon, daß Menschen unter ihre E-Mails ein paar Vokabeln wie „Bombe“, „Anschlag“, „geheim“ etc. geschrieben haben, um damit die Überwachung auf Trab zu halten und gegen die totale Speicherung zu protestieren. Natürlich halte ich nichts davon, sich jetzt irgendwie einzuschränken – letzten Endes ist doch der Kontrollwahn der Innenpolitikerinnen der direkte Weg ins Orwell‘sche 1984, permanente Angst und damit Konformität. Nichts mehr zu sagen und dann zu hoffen, daß es dich nicht trifft, ist eine nachvollziehbare Reaktion, die nur leider nichts nützt. Erstens macht es keinen Spaß, ein Leben in permanenter Angst davor zu leben, daß du doch irgendwie auffällst, und zweitens ist jetzt wohl ziemlich deutlich geworden, daß wir selber nicht wirklich beeinflussen können, ob wir in die Raster geraten. Und das einzige, was hilft, ist meiner Ansicht nach, laut und deutlich zu sagen, daß uns das


Stasi 1.0

nicht gefällt. Wenn das nicht mehr geht, ist es einfach alles zu spät.

Lars Sobiraj: Wenn, wie kürzlich geschehen, euch am selben Tag auf völlig unterschiedlichen Streckenabschnitten in der Straßenbahn der gleiche Beamte begleitet, kann dies zumindest als sehr ungeschickt bezeichnet werden. War die Observierung vom BKA schlichtweg tolpatschig organisiert oder vermutest du dahinter eine andere Absicht – so quasi als Hinweis: Eure Familie befindet sich noch immer im Fokus der Ermittlungen?

Anne: Darüber habe ich in letzter Zeit mit vielen Leuten geredet. Ich glaube, daß das Absicht ist. Das BKA ist ja keine Anfänger-Behörde, die stecken vermutlich relativ viel Geld in Ausbildungs- und Personalkosten. Die lange Geschichte bringt wohl auch allerhand Erfahrung mit, würde ich denken. Verdeckte Ermittlungen sollen schon an sich eben das sein: verdeckt. Und wenn sie wollen, dann schaffen sie das sicher. Deswegen denke ich, daß es darum geht, uns ein bißchen verrückt zu machen. Gleichzeitig sind gerade die technischen Pannen teilweise so komisch, daß ich mir vorstellen kann, daß ihnen das vielleicht gar nicht klar ist, wie sich manche Sachen auswirken – normalerweise kriegen sie vielleicht nicht soviel Feedback? Vielleicht sollten wir mal fragen, ob wir das bezahlt kriegen können..

Lars Sobiraj: Ich fand es unglaublich mutig, die Verfolger durch deine Veröffentlichungen ein Stück weit selbst zu beobachteten und zu Verfolgten zu machen. Viele Menschen würden sich in der gleichen Situation aus Angst einfach in sich und ihre vier Wände zurückziehen und sonst nichts tun. Welche konkreten Auswirkungen hatte und hat die Überwachung auf euer Leben? Achtet ihr noch immer vermehrt auf das, was ihr tut und sagt? Oder ist einem das irgendwann egal, weil man vielleicht im Laufe der Zeit eine Art Trotzhaltung angenommen hat?

Anne: Mir ist es immer noch ständig sehr bewußt, daß sie da sind. Ich weiß ja z. B. nicht, ob in unserer Wohnung Wanzen sind, und wenn ja, wo. Das Gefühl, daß da permanent wer zuhört, ist sehr unangenehm. Ich weiß inzwischen, daß die Telefonate nicht aufgezeichnet werden, sondern da immer Leute live sitzen und zuhören. Das völlig zu ignorieren, schafft wahrscheinlich niemand. Es beeinflußt mich nicht mehr so stark wie am Anfang, was auch damit zu tun hat, daß ich das Gefühl habe, daß sie Andrej jetzt nicht mehr wirklich als Terroristen für Jahre in den Knast stecken können. Das war am Anfang anders. Die öffentliche Reaktion und dann die Entscheidung des Bundesgerichtshofes haben dabei sehr geholfen. „Trotzhaltung“ trifft es vielleicht ganz gut. Ich habe wochenlang darüber nachgedacht, ob ich anfange zu bloggen. Natürlich hatte ich Angst vor der Reaktion – halten mich alle für paranoid? Was machen BKA und Verfassungsschutz? Von Spam-Bombardements bis zu einer Gegenreaktion in rechten Publikationen habe ich mit allem gerechnet. Außerdem befand ich mich ja vorher in der nicht ganz so schrecklichen Rolle, bloß „die Freundin von“ zu sein, die nach Aktenlage für die Behörden völlig unbekannt und uninteressant ist. Jetzt zeige ich relativ deutlich, daß ich auch denken kann und mich nicht in der Regel unter dem Tisch verstecke, und ich war mir nicht so sicher, wohin daß heutzutage führt.

Inzwischen mache ich auch das Handy wieder ab und zu aus, wenn ich nicht will, daß sie zuhören. Und merke, daß Bloggen das beste war, was ich tun konnte, weil ich fast ausschließlich sehr positive und unterstützende Reaktionen kriege. Das macht es einfacher, mit der Situation fertigzuwerden, und mir persönlich geht es auch einfach viel besser damit, das alles nicht runterzuschlucken und nur mit mir alleine auszumachen. Kann ich nur dringend empfehlen, und machen jetzt ja auch mehr Leute.

Bisher war es, glaube ich, immer so, daß Linke, die solche Verfahren hatten, innerlich so eine Art Ritterrüstung angezogen haben und sich jenseits von sehr starren Erklärungen öffentlich gar nicht mehr geäußert haben. Ich halte das für falsch. Für mich ist das kein Zweikampf zwischen Beschuldigten und Behörden, sondern ein Kampf, der nur mit (also: in) der gesamtem Gesellschaft geführt werden kann – ein sehr

politischer Kampf, um es mal ganz pathetisch auszudrücken, um Meinungen, Deutungshoheit, die politische Richtung und letzten Endes, jetzt noch pathetischer, um Macht. Die Waffen sind hier ein bißchen ungleich verteilt, aber das heißt nicht, daß wir es nicht versuchen sollten. Und es gehört zu meinen Grundüberzeugungen, daß für gesellschaftliche Veränderungen alle Menschen „mitkommen" müssen, und der erste Schritt dazu sind immer öffentliche Debatten.

Lars Sobiraj: Wieviel kann man deiner Meinung nach mit der Publikation persönlicher Eindrükke in einem Weblog wirklich bewegen? In der heutigen Zeit hat viele Bundesbürgerinnen eine umfassende Trägheit und Gleichgültigkeit erfaßt. Viele denken, daß sie sowieso nichts ausrichten können.

Anne: Naja, ich bilde mir nicht ein, daß mit Blogs wirklich viel verändert wird. Sie sind im besten Fall ein Teil öffentlicher Auseinandersetzung. Die Blogosphäre ist immer noch eine relativ exklusive Angelegenheit, deswegen würde ich das nicht überbewerten. In meinem Fall war die Wirkung ziemlich weitreichend, was natürlich damit zu tun hat, daß ein Terrorismusverfahren in Zeiten von Vorratsdatenspeicherung & Co einfach sehr viel Aufmerksamkeit erhält. Die Nahaufnahme, der direkte Blick in Terroristens Wohnzimmer, hat sicher eine Rolle gespielt, und der Gruselfaktor ist ja auch nicht unerheblich. Schreiben können hilft sicher auch. Ich finde, daß Bloggen eine gute Möglichkeit ist, die eigene Meinung unzensiert öffentlich zu machen. Wieviel das gegen die Trägheit vieler Menschen gegenüber der Überwachungsgesellschaft ausrichten kann, in der wir ja de facto schon leben, kann ich auch nicht sagen. Ich bin nicht sehr optimistisch, andererseits bin ich natürlich dafür, es zu versuchen, denn alles andere ist auch nicht wirklich eine Alternative. Ich glaube aber auch, daß am Computer sitzen alleine nicht viel ändern wird.

Bezüglich der Besucherzahlen: Am Anfang hatte ich ca. 4.000 bis 5.000 Besucher auf meinem Weblog, ein Artikel erreichte sogar knapp 15.000, glaube ich. Inzwischen hat es sich bei 400 bis 500 eingependelt, mit Ausnahme eines Artikels, der sich nicht mit Überwachung, sondern nackten Frauen beschäftigt, und da sind's inzwischen über 1000. (lacht)

Lars Sobiraj: Die netzaffinen Spatzen haben von den Dächern gepfiffen, daß eure Preisverleihung Ende Dezember auf dem Chaos Communication Congress stattfinden sollte. Habt ihr vom Bündnis für die Einstellung des Paragraphen 129a bereits spannende Einsendungen bezüglich der Definition von Terrorismus

erhalten? Gibt es schon einen Favoriten innerhalb der Jury?

Anne: Oh je. Wir hatten beschlossen, die Preisverleihung zu verschieben, weil die Beteiligung doch etwas träge ist und andererseits allerhand Leute signalisiert haben, daß sie noch Zeit brauchen. Und weil wir nach den letzten vier Monaten auch etwas aus der Puste sind. Ich habe aber beim Congress über mein Leben als „Frau vom Terroristen-Andrej" (Zitat Fefe) erzählt. Das war eine sehr nette Einladung: Eine Stunde im großen Saal, ich war durchaus ein bißchen aufgeregt. Und das Preisausschreiben läuft also noch ein bißchen weiter. Wir haben schon allerhand Einsendungen, (fast) alle auf der Webseite zu sehen. Das ist **die** Gelegenheit, sich nochmal Gedanken zu machen und was Hübsches einzureichen. Wir freuen uns auch weiter über attraktive Preisspenden!


Foto: Thomas Pirot

Lars Sobiraj: Gibt es Überlegungen, irgendwann in den nächsten Jahren auszuwandern, wenn sich der Wind gelegt hat?

Anne: Um Gottes Willen! Geht gar nicht – ich glaube, wenn Andrej auch nur daran denken würde, würden sie ihn wahrscheinlich wegen Fluchtgefahr sofort wieder festnehmen. Im Ernst: Können wir nicht, weil ja vorläufig immer noch ein Verfahren läuft gegen ihn, das ihn dann jetzt wohl beschuldigt, einer kriminellen Vereinigung anzugehören. Abgesehen davon wüßte ich auch nicht wirklich wohin, denn in den meisten anderen Staaten, deren Sprachen ich kann, sieht es nicht so viel besser aus, oder ich würde aus anderen Gründen da nicht hin wollen. Und schließlich ist es mit einem Stadtsoziologen, der am besten deutsch kann und als Terrorist verschrien ist, auch nicht so einfach, umzuziehen. Vielleicht sollten wir Lotto spielen...

Lars Sobiraj: Anna, zunächst vielen Dank dafür, daß du dir so viel Zeit für uns genommen hast. Dir und deiner Familie wünsche ich weiterhin viel Kraft und Mut, um die seit Monaten anhaltende Situation möglichst schadlos überstehen zu können. Ich bin nach dem Studium deines Blogs ebenfalls ins Grübeln gekommen. Nachdem man eure Geschichte verfolgt hat, wird man bei Zwischenfällen plötzlich skeptisch, die man vorher nur als technisches Versagen abgetan hätte. Paranoia sollte als Folge nicht plötzlich ausbrechen. Aber vielleicht kann man als Außenstehender der ganzen Angelegenheit doch etwas Positives abgewinnen. Wenn die Geschichte von Anne und Andrej dazu beigetragen konnte, daß wir über die Methoden der Ordnungshüter jetzt kritischer nachdenken als zuvor. In dem Fall könnte man sagen, der Vorfall war zumindest nicht ganz umsonst.

Anm. d. Redaktion: Annes Blog findet ihr unter *http://annalist.noblogs.org/*

BigBrotherAwards 2007

Lars Sobiraj

Am 12. Oktober 2007 war es wieder soweit: Der FoeBuD e. V. und sechs weitere Organisationen haben die Datenschützer des Landes in den Nordosten von Nordrhein-Westfalen geladen. Rund 400 Interessierte und zahlreiche Vertreter der Presse sind der Einladung gefolgt.

Und wie fast jedes Jahr im Herbst wollte keiner der Preisträger seine Auszeichnung in Empfang nehmen. Langweilig ist es im Dachgeschoß der Ravensberger Spinnerei trotzdem nicht geworden. Die Jury hat in monatelanger Arbeit die Schwemme der eingereichten Hinweise für jede einzelne Kategorie überprüft. Bei über 500 Benennungen hatte man es sehr schwer, die richtigen Überwacher, Bespitzelnde und Datensammler herauszufiltern. Beunruhigend ist in jedem Fall: Die Zahl der Nominierungen wächst von Jahr zu Jahr stetig an.

Arbeitswelt – Keine Gefangenen machen!

Beginnen wollen wir mit der Kategorie Arbeitswelt. Hier räumt die Novartis Pharma GmbH den Preis für die systematische Bespitzelung ihrer Außendienstmitarbeiter durch Detektive und eine vorsätzliche Verletzung der zugesicherten Anonymität bei internen Erhebungen ab. Das Pharmaunternehmen hat ihren Außendienstmitarbeitern in großem Stil Detektive hinterhergeschickt.

Man wollte überprüfen, ob diese die bilanzierten Arzt- und Apothekenbesuche auch wirklich durchgeführt haben. In diesem Arbeitsbereich scheint tatsächlich der Kriegszustand ausgebrochen zu sein. So gab der Geschäftsführer der Konzernmutter die kernige Parole aus: „Kill To Win – No Prisoners“. Es stellt sich die Frage, ob Personen Höchstleistungen erbringen, nur weil sie das Gefühl nicht loswerden, überwacht zu werden.

Qualifiziert für den BBA hat sich das Unternehmen auch durch die Rückgabe „anonymer“ Umfragen im Kollegenkreis. Diese sind, nachdem sie nachträglich personalisiert wurden, direkt bei der Personalabteilung gelandet. Später wurden den überraschten Mitarbeitern die eigenen Umfrageergebnisse inklusive ihres Namens zurückgegeben. Die für die Umfrage beauftragte Agentur kommentierte die Angelegenheit mit den Worten: „So naiv kann man doch nicht sein!“ Warum Anonymität aufrechterhalten, die man zuvor ausdrücklich zusicherte? Fast erscheint es, der Zweifrontenkrieg in diesem Sektor wird gegen die eigenen Reihen und nicht gegen die Konkurrenz geführt.

Der Betriebsrat sah sich immerhin genötigt, die Bespitzelung durch die Detektive offenzulegen. Es gab leider keine sichtbaren Anzeichen für Bemühungen, die eigenen Mitarbeiter zu beschützen. Es scheint fast so, als wenn Herr Dr. Maag, der Vorstandsvorsitzende des Unternehmens, dort alles und jeden gut im Griff hat. Wie auch immer: Unser herzliches Beileid zum BigBrotherAward 2007!

Behörden und Verwaltung – Der Duft des Terrors

In der Kategorie Behörden und Verwaltung hat sich die Generalbundesanwältin Monika Harms durch ihre Maßnahmen gegen die Gegner des G8-Gipfels in Heiligendamm im Mai dieses Jahres besonders hervorgetan.

Zum einen hat sie beim Ermittlungsrichter beantragt, trotz des Briefgeheimnisses auf der Suche nach Bekennerschreiben in Hamburg systematische Kontrollen von tausenden von Briefen durchzuführen. Andererseits ordnete sie an, von Gipfelgegnern Geruchsproben zu nehmen und diese zu konservieren. Die Mitarbeiter von Frau Harms haben jedoch bislang keinen einzigen Terroristen ermitteln können. Die Geruchsproben sollten bestimmen, ob sich ein Verdächtigter an einem bestimmten Ort aufgehalten oder ein Tatwerkzeug bzw. ein Bekennerschreiben berührt hat.


GBA Monika Harms

„Stinknormal“ kann man das nicht mehr nennen. Selbst dem als sicherheitspolitischen Scharfmacher geltenden SPD-Politiker Dieter Wiefelspütz ging das zu weit, er sagte über Frau Harms: „Sie ist auf den Hund gekommen und sollte so schnell wie möglich davon wieder runterkommen.“

Regional – Hamburgs Schulen als neue Abschiebebehörden?

Der BigBrotherAward in der Kategorie „Regional“ geht dieses Jahr an Frau Senatorin Alexandra Dinges-Dierig, respektive an die Behörde für Bildung und Sport der Freien und Hansestadt Hamburg.

Deren „Verdienst“ ist die Einrichtung eines Schülerzentralregisters mit dem Nebenzweck, ausländische Familien ohne Aufenthaltserlaubnis aufzuspüren.

Die Schulpflicht einerseits und das verbriefte Recht von Kindern auf Bildung andererseits sorgen für eine lückenlose Erhebung aller Schülerdaten der Schulen der Hansestadt. Es erfolgt ein automatischer Abgleich mit dem Melderegister, um den illegalen Aufenthalt von Kindern und ihren Eltern festzustellen. Offiziell wird diese Handhabe damit begründet, daß man tragische Fälle verhindern will, bei denen Kinder wegen Mißhandlung oder Vernachlässigung durch ihre Eltern über einen längeren Zeitpunkt der Schule ferngeblieben sind.


Alexandra Dinges-Dierig

Als Folge schicken viele illegale Einwanderer aus Angst ihre Kinder erst gar nicht zur Schule, weil sie dadurch ihre Aufdeckung befürchten. Ein Gesetz, welches dem Schutz der Kinder dienen sollte, sorgt somit für weniger Schüler im Klassenzimmer und auch für weniger Bildung.

Wirtschaft – Anonymes Reisen mit der Bahn unerwünscht

Die Provisionen für Reisebüros wurden systematisch gekürzt, was dazu geführt hat, daß die Karten für die Deutsche Bahn nur noch vom Unternehmen selbst angeboten werden.

Wer sein Ticket anonym am Schalter erwerben will, muß viel Zeit und Geduld mitbringen. Bis zu fünf Euro im Vergleich zu den Online-Angeboten kostet den Bahn-Kunden die Wartezeit am Schalter extra. Bucht man über das Internet, ist man dem „Unternehmen Zukunft“ mit Namen, Adresse und Bankverbindung bekannt. Viele Automaten in den Bahnhöfen nehmen nur EC-Karten und kein Bargeld an, was einem erneut das anonyme Reisen unmöglich macht.

Um die Preisnachlässe mitnehmen zu können, wird vom Automaten das Einführen der Bahncard verlangt. Unbegreiflich ist diese Vorgehensweise primär deshalb, weil die Rabattansprüche sowieso erst bei der Fahrkartenkontrolle im Zug überprüft werden. Dazu kommt die überflüssige Angabe des Geburtsdatums und das Foto auf der Bahncard. Was man mit den bio-

metrischen Daten der Kunden anstellen kann – bedenkt man die flächendeckende Videoüberwachung des Bahngeländes – man mag es sich besser nicht ausmalen.

Im Fall der „Bahncard 100“ ging man absolut auf Nummer sicher. Die Bahn integrierte in jede „Bahncard 100“ fast unbemerkt einen RFID-Schnüffelchip. Wären die Lesegeräte für solche Chips so flächendeckend aufgestellt wie geplant, könnte die Bahn problemlos jeden Schritt des Reisenden überwachen und protokollieren. Im Sinne der Data-Miner – gut gemacht!
Wir können dem Vorsitzenden des Vorstands der Deutschen Bahn AG, Herrn Mehdorn, nur zu seiner Datensammelwut und seinem Preis gratulieren.

Verbraucherschutz – lukrative Hotelgäste von Billigurlaubern unterscheiden

Stellvertretend für viele, viele weitere Ketten erhalten die Hotelketten Marriott, Hyatt und Intercontinental den BBA für die Kategorie Verbraucherschutz.

Viele Hotels speichern die Vorlieben und Daten ihrer Gäste, um diese später besser differenzieren zu können. Hat der Gast Telefonate in den Mittleren Osten durchgeführt? Besteht eine Haselnußallergie? Hat er sich via Pay-TV Pornos in sein Zimmer übertragen lassen? Die Tentakel der Gastlichkeit tragen die Daten zusammen, wie etwa Familienkonstellationen, Trink-, Rauch- und Eßgewohnheiten, Allergien, Hobbies, Sonderwünsche, Beschwerden, Vorlieben etc.

Es geht dabei nicht primär – wie man denken könnte – um eine optimale Versorgung der Gäste. Das Zauberwort lautet CRM, das „customer relationship management“. Dabei sollen die Sparsamen von den spendablen Gästen unterschieden werden. Diejenigen mit Spendierhosen möchte man später noch einmal gesondert ansprechen. Wie aber geht man nach der Auswertung der Daten mit den preisbewußten Kurzurlaubern um?

In Frankreich werden die persönlichen Daten von der Hotelkette direkt an die Polizei übertragen. Auch Geheimdienste könnten sich für Telefonate nach Syrien, den Verzehr von Schweinefleisch oder Gäste aus dem Iran interessieren. Viele der konzerneigenen Server europäischer Hotelketten stehen in den USA. Und spätestens seit dem „patriot act“ ist es Mitgliedern der amerikanischen Geheimdienste ohne richterlichen Beschluß erlaubt, diese Daten einzusehen und auszuwerten.

König Kunde indes schläft hoffentlich ruhig und sanft. Er hat von alledem keinen blassen Schimmer. Friedrich Schiller würde dies wahrscheinlich mit den Worten kommentieren: „Hier wendet sich der Gast mit Grausen. So kann ich hier nicht ferner hausen.“

Technik – lückenlose Totalüberwachung im Auto

Im Bereich Technik geht der Preis dieses Jahr an die Firma PTV Planung Transport Verkehr AG für ihr sogenanntes „Pay-as-you-drive“-System.

Dies ist ein Gerät, welches automatisch die Fahrroute und das Fahrverhalten des Fahrers aufzeichnet und die Daten ohne Zeitverzögerung per Mobilfunk an die Versicherung übermittelt. Das Verfahren soll mit der Begründung eingeführt werden, daß vernünftig und umsichtig fahrende Personen niedrigere Versicherungsprämien zahlen müssen als andere.

Über den Geldbeutel sollen vor allem Fahranfänger zu mehr Vernunft, leider auch zu mehr Kontrolle am Steuer bewegt werden. In Zeiten, in denen viele PKW über Bordcomputer verfügen, kann man Beschleunigungssensoren anzapfen, kontrollieren, ob geblinkt wurde, sogar der Reifendruck und der Alkoholgehalt des Atems des Fahrers könnte überprüft werden. Wenn das selbst verordnete sanfte Fahrverhalten mit den gesammelten Daten übereinstimmt, bleibt die Prämie niedrig, ansonsten müssen die Fahrer mit höheren Versicherungsbeiträgen rechnen. Auch das Einhalten gesetzlich angeordneter Verbote könnte überprüft oder gar elektronische Strafzettel ausgestellt werden.

Die Vorstellung, Herr über diese Daten zu werden, wäre für den Gesetzgeber sicherlich sehr verlockend. Man denke nur an die schleichende Veränderung der gesetzlichen Grundlagen, wenn es um die Mautdaten geht. Anfangs hat kein Politiker offen über eine Verwendung der Mautdaten zu Fahndungszwecken gesprochen. Heute sieht die Praxis – dank frischer Gesetze in den Ländern – ganz anders aus.

Wie also fühlen Sie sich bei der Vorstellung, wenn dieses System in ein paar Jahren eingeführt wird und sich die Polizeibeamten virtuell auf ihr Gerät aufschalten dürfen? Sie könnten dann feststellen, wo sich das überwachte Auto befindet, wie schnell und in welche Richtung es fährt. Auch nach Monaten könnte noch immer ein Bewegungsprofil erstellt werden. Und selbst, wenn dieser elektronische Big Brother die Kosten für die Versicherung deutlich senken könnte, werden sich so manche Fahranfänger genauer überlegen müssen, wie viel ihnen ihre Unabhängigkeit wert ist.

Politik – Dank Steinbrück Steuer-ID ab Geburt bis 20 Jahre nach dem Tod

Der BBA in der Kategorie Politik geht an den Bundesminister der Finanzen, Herr Peer Steinbrück, für die Einführung der lebenslangen Steueridentifikationsnummer (Steuer-ID) für alle Einwohnerinnen und Einwohner der Bundesrepublik Deutschland.

Die Steuer-ID wird ab Geburt vergeben und ist bis 20 Jahre über den Tod des katalogisierten Steuerzahlers hinaus gültig. Dadurch soll eine eindeutige Identifizierung des Steuerpflichtigen im Besteuerungsverfahren erreicht werden. Wenn in nicht allzu ferner Zukunft diese Nummer mit den von Überwachungskameras erhobenen Daten – und der damit einhergehenden Identifikation der gefilmten Personen per Biometrie – kombiniert werden kann, ist es bis zur Fiktion von George Orwell nicht mehr allzu weit entfernt.


Bundesfinanzminister Peer Steinbrück

Die staatliche Schlinge um den Hals der beäugten Bürgerinnen und Bürger scheint sich immer mehr zuzuziehen.

Kommunikation – Das ewige Thema Vorratsdatenspeicherung

Frau Bundesministerin der Justiz Brigitte Zypries wird ausgezeichnet für ihren Gesetzentwurf, mit dem in Deutschland die Vorratsdatenspeicherung von Telekommunikations-Verbindungsdaten für sechs Monate durchgeführt werden soll.

Auch SPD: Brigitte Zypries, Bundesministerin der Justiz

Sie ignorierte damit bewußt die Rechtsprechung des Bundesverfassungsgerichts, das bereits 1983 im Volkszählungsurteil festgelegt hatte, daß die Sammlung von nicht anonymisierten Daten zu unbestimmten oder noch nicht bestimmbaren Zwecken mit dem Grundgesetz unvereinbar ist. Auch die Nichtigkeitsklage von Irland vor dem Europäischen Gerichtshof hat die Ministerin nicht von ihrem Vorhaben abhalten können. Abschließend sollte man noch kurz erwähnen, daß Frau Zypries wegen des Großen Lauschangriffs schon vor drei Jahren mit einem BBA ausgezeichnet wurde.

Schäuble: Trotz enorm viel Fleiß': Kein Preis!

Außer Konkurrenz lief dieses Jahr der absolute Traumkandidat der Awards: Bundesinnenminister Wolfgang Schäuble. Nach Ansicht der Jury wäre es falsch, sich zu sehr auf diesen überqualifizierten Bewerber einzuschießen. Andererseits befürchtet man, Schäuble könnte seine Auszeichnung als besonderen Ansporn verstehen und seinen Sicherheitsextremismus und Terrorwahn noch weiter ausdehnen. Auch mußte man ihm dankbar zugute halten, daß er im September für eine erfolgreiche Demonstration in Berlin gesorgt hat. Schäuble hat wie kein anderer Politiker für ein vermehrtes Bewußtsein dieser Problematik in der Bevölkerung gesorgt und hat die Menschen wie kein Zweiter auf die Barrikaden gehen lassen.

Fazit

Der Titelverteidiger ging diesmal leer aus: Darth Schäuble, Chefinternetausdrucker und Bestimmer im BMI

In manchen Kategorien war die Vergabe der Awards schon im Vorfeld absehbar, andere wurden zur allgemeinen Überraschung verliehen. Insgesamt war es – wie auch letztes Jahr – eine Veranstaltung, die in sich rund wirkte. Den Zuschauern wurde erneut eine zweistündige Gala geboten, die viele interessante Informationen und einiges an kurzweiligem Entertainment im Angebot hatte. Das Verhältnis anwesender Presse zu Zuschauern schien sich in Richtung Kameramänner, Kabelträger und Journalisten verschoben zu haben. Auch wenn der Saal keinen erheblichen Zuwachs von Teilnehmern erlaubt: Bei diesem spannenden Themenspektrum könnte es ruhig mehr Menschen in die Bielefelder Innenstadt verschlagen. Und auch eine Berichterstattung durch mehr Mainstream-Medien wie Nachrichtenmagazine, Hörfunk und TV wäre sehr wünschenswert.

Wichtig ist der mahnende Zeigefinger der BBA-Jury allemal. Wer sonst erinnert einen jährlich daran, wie viel Schindluder mit unseren höchst sensiblen Daten betrieben wird. Und für die Organisatoren gilt: Nach der Veranstaltung ist vor der Veranstaltung. An eine lange Verschnaufpause war nicht zu denken. In der Zwischenzeit sind die Vorbereitungen für die Preisverleihung der Datenkraken für das Jahr 2008 längst angelaufen.

Nicht unter den Verurteilten: padeluun im Gespräch mit Andreas Liebold

Piling more hay

von Constanze Kurz <46halbe@weltregierung.de>

Es war im Frühjahr 2004 im Europäischen Rat, die Debatten über die Harmonisierung der Mindestspeicherungspflichten von Telekommunikationsdaten ist in vollem Gange. Es gibt Vorschläge aus Frankreich, Irland, Schweden, Großbritannien, die Diskussionen werden kontrovers geführt. Nur in einem sind sich alle Teilnehmer einig: Die Strafverfolgung muß effektiver gestaltet werden.

Muß sie das tatsächlich?

Eine wirksame Strafverfolgung ist eine wesentliche Aufgaben der Staaten. In den letzten Jahren hat sich jedoch gezeigt, daß die Wirksamkeit beschlossener Gesetze kaum noch oder gar nicht unabhängig überprüft wird. Die Vorratsdatenspeicherung ist auch deshalb kritisiert worden, da neben schwerwiegenden verfassungsrechtlichen Bedenken die Effektivität der Maßnahme schon im Vorfeld der Beschlüsse fragwürdig erschien. Mit dem Vorhaben werden Telekommunikationsanbieter europaweit verpflichtet, Daten etwa zum Zwecke der Strafverfolgung zu speichern. Bisher war es ihnen in geringerem Umfang lediglich zu Abrechnungszwecken **gestattet**.

Die britische EU-Ratspräsidentschaft setzte die Richtlinie zur Vorratsdatenspeicherung gegen die Haltung vieler kritischer Mitgliedstaaten durch. Damit war die Speicherungspflicht für die Telekommunikationsverkehrsdaten europaweit faktisch besiegelt. Der einige Wochen später folgende Ratsbeschluß war nur noch Formsache.

Die Richtlinie sieht konkret vor, dass die Verbindungsdaten vom Provider in einem Zeitraum von mindestens sechs Monaten bis maximal zwei Jahren gespeichert werden müssen. Anders als EU-Verordnungen treten Richtlinien nicht direkt in den europäischen Ländern in Kraft. 18 Monate Frist räumte die EU den Mitgliedsstaaten ein, um die Beschlüsse in nationales Recht umzusetzen. In Deutschland bedurfte es hierzu einer Änderung des Telekommunikationsgesetzes. Es ist der mittlerweile altbekannte Umweg über die EU, der eine parlamentarische und gesellschaftliche Debatte von vorneherein ad absurdum führte.

Über die Rechtmäßigkeit der Richtlinie wird der Europäische Gerichtshof entscheiden, erheb-

liche Zweifel sind angebracht. Da die Gesetzgebung in Deutschland jedoch bereits angepaßt wurde, wird die gerichtliche Entscheidung hierzulande keine direkte Wirkung haben.

Natürlich darf in Deutschland auf die Daten legal nur nach richterlichem Beschluß zugegriffen werden. Aber wirft man einen Blick auf die vergangenen Jahre und die tatsächlichen Prüfungen von Richtern, wird man entdecken, daß dies kaum Schutz vor Mißbrauch bietet. Vor allem überforderte Amtsrichter, die in schöner Regelmäßigkeit vom Bundesverfassungsgericht bescheinigt bekommen, daß sie die Verfassung mißachten, werden sich sicher in Zukunft nicht als ernstzunehmende Grundgesetzverfechter entpuppen.

Hinzu kommt, daß sich im Zuge einer hysterischen Berichterstattung nach dem Motto "Terror lauert immer und überall" nach und nach auch das Bewußtsein für den Grundsatz der Verhältnismäßigkeit ändert. Daß es gerade in Deutschland tatsächlich dazu gekommen ist, Vorhaben in die Tat umzusetzen, die es erlauben, die Telekommunikationsdaten von über 80 Millionen Menschen verdachtsunabhängig zu speichern, zeugt von einem Paradigmenwechsel. Auch wenn in Europa die Richtlinie gekippt wird und das deutsche Gesetz vor dem Bundesverfassungsgericht keinen Bestand haben wird: Ein Dammbruch bleibt es allemal.

Erstaunlich ist, wie schnell sich die Folgen der Gesetzgebung konkret zeigen. Bereits einen Monat nach Inkrafttreten entfaltet die Vorratsdatenspeicherung ihre unheilige Wirkung, obgleich ja technisch noch wenig umgesetzt wurde. Auf zwölf Seiten faßt der Anwalt Meinhard Starostik, der vor dem Bundesverfassungsgericht die Verfassungsbeschwerde im Namen von tausenden Bürgern eingelegt hat, zusammen, was eine Befragung von 8.000 Personen nach dem Inkrafttreten ergeben hat – ein Dokument einer sich nachhaltig verändernden Gesellschaft. [1]

Die Logik, mit der wie bei einem Pawlowschen Reflex nach jedem Anschlagsversuch neue Sicherheitsmaßnahmen gefordert werden, wird noch immer zu wenig hinterfragt. Bei der Vorratsdatenspeicherung waren etwa die Daten des Handys eines der Verdächtigen des Anschlags in Madrid ein immer wieder vorgebrachtes Argument. Die Kenntnis der Verbindungsdaten kann natürlich einen solchen Anschlag nicht verhindern, sie kann maximal der Aufklärung dienen. Auch ein Präventiveffekt ist nicht anzunehmen, da mit der Vorratsdatenspeicherung anlaßlos jede Verbindung gespeichert wird. "We're looking for a needle in a haystack here and he is just piling on more hay", warf Al Gore dem damaligen US-amerikanischen Justizminister John Ashcroft vor. Letztlich wird auch die Vorratsdatenspeicherung zu einem Verlust an Sicherheit führen: Denn unhaltbare Sicherheitsversprechen zerstören, was sie vorgeben zu schützen.

[1] *http://www.vorratsdatenspeicherung.de/images/schriftsatz_2008-01-31_anon.pdf*

Vorratsdatenspeicherung

Ein Ermittlungsinstrument ohne Alternative?

von Dr. Marco Gercke

Die Neueinführung von strafprozessualen Ermittlungsinstrumenten oder deren Erweiterung hat seit jeher den Stoff intensiver Debatten innerhalb von Gesellschaft, Politik und Justiz geliefert. Beispiele dafür sind der „Große Lauschangriff" ebenso wie die Telefonüberwachung.

Die Intensität der Debatten ist insoweit nicht weiter verwunderlich, als strafprozessuale Maßnahmen zu den intensivsten Eingriffen im Verhältnis von Staat und Bürger zählen. Der Protest gegen die obengenannten Maßnahmen zog sich quer durch Gesellschaft. So erklärte die damalige Bundesministerin der Justiz, Sabine Leutheusser-Schnarrenberger, 1995 aus Protest gegen die Unterstützung des Gesetzesvorhabens „Großer Lauschangriff" durch ihre Partei ihren Rücktritt.

Ebenso wie der Protest gegen die Ausweitung staatlicher Befugnisse zu den Reaktionen auf die Einführung neuer Ermittlungsinstrumente zählt, folgt ihrer Einführung nicht selten eine Überprüfung durch die Gerichte, verbunden mit einer Entscheidung durch das Bundesverfassungsgericht. So hat das höchste deutsche Gericht in einer Entscheidung aus dem Jahr 2004 hinsichtlich des „Großen Lauschangriffs" ausgeführt: „Die Vorschriften der Strafprozeßordnung zur Durchführung der akustischen Überwachung von Wohnraum zu Zwecken der Strafverfolgung genügen den verfassungsrechtlichen Anforderungen [...] nicht in vollem Umfang." [1]

Im Zuge der gesetzgeberischen Maßnahmen als Reaktion auf die Anschläge vom 11. September 2001 in New York hat die Dynamik der Diskussion um die Einführung neuer Ermittlungsinstrumente deutlich zugenommen. Vor dem Hintergrund der Bekämpfung des internationalen Terrorismus wurden sowohl im Bereich der Gefahrabwehr als auch der Strafverfolgung mehrere Gesetze verabschiedet, welche die Befugnisse der staatlichen Organe erweiterten. Nicht selten entstand im Rahmen der hektischen legislativen Betriebsamkeit der Eindruck, daß das Ziel (die Bekämpfung des Terrorismus) dabei bisweilen als Ersatz für die notwendige Rechtfertigung neuer Eingriffsbefugnisse diente. Während dies vor dem Hintergrund der zeitlichen Nähe der Anschläge für die ersten Gesetzesinitiativen zumindest nachvollziehbar erscheint, verwundert es doch, daß der Trend, Gesetze eher auf Prognosen als auf verläßliche Erkenntnisse zu stützen, auch fast sechs Jahre nach den Anschlägen anhält.

Wertungswidersprüche im Zusammenhang mit Strafnormen aus dem Bereich des Internetstrafrechts

Vergleicht man die jüngeren Gesetzgebungsverfahren im Bereich des Internetstrafrechts mit legislativen Ansätzen außerhalb des Internet, so drängt sich bisweilen der Eindruck auf, daß die Kriminalisierung von Vorgängen im Internet erheblich weiter fortgeschritten ist. Verdeutlicht werden soll dies an zwei Beispielen. Vorab sei darauf hingewiesen, daß es für jede einzelne Maßnahme – für sich betrachtet – eine Begründung gibt. Die Kritik setzt daher nicht an den Einzelmaßnahmen, sondern an der Richtungswirkung der Summe der Einzelmaßnahmen an.

a) Ein Beispiel ist die Strafbarkeit von Vorbereitungshandlungen. Gemäß dem neu eingeführten § 202c StGB macht sich strafbar, wer ein Computerprogramm, dessen Zweck die Bege-

hung einer Computerstraftat ist, herstellt. Wer hingegen Küchenmesser herstellt, die zur Begehung schwerer Körperverletzung verwendet werden können, macht sich – sofern nicht weitere Handlungen hinzutreten – nicht strafbar.

b) Die ungleiche Behandlung von Handlungen innerhalb und außerhalb des Internet läßt sich ferner an der Regelung in § 263a Abs.3 StGB verdeutlichen. Gemäß § 263a Abs.3 StGB macht sich strafbar, wer ein Computerprogramm herstellt, dessen Zweck die Begehung eines Computerbetrugs ist. Eine vergleichbare Vorbereitungshandlung eines klassischen Betrugs – z. B. die Manipulation von Spielkarten zum späteren Einsatz – ist nicht strafbar.

Die Ungleichbehandlung beschränkt sich nicht auf die Einführung von Strafvorschriften, sondern wird auch im Bereich des Strafprozeßrechts deutlich. Auch hier soll die Ungleichbehandlung anhand eines Beispiels verdeutlicht werden.

c) Nach der Entscheidung des Bundesgerichtshofs über die fehlende Rechtsgrundlage für die Durchführung von heimlichen Online-Durchsuchungen wird derzeit intensiv an der Einführung eines entsprechenden Ermittlungsinstruments gearbeitet. Sofern das Instrument nicht nur beim Verdacht besonders gravierender Straftaten eingesetzt werden soll, entsteht ein Wertungswiderspruch zu den außerhalb des Internet zur Verfügung stehenden Ermittlungsmaßnahmen. Dort ist ein Zugriff auf Gegenstände in der Wohnung des Verdächtigen grundsätzlich nur im Wege einer offen durchgeführten Durchsuchung, nicht aber durch einen heimlichen Zugriff zulässig.

Die EU-Richtlinie zur Vorratsdatenspeicherung, die mit dem Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen umgesetzt werden soll, setzt die oben dargestellten Wertungswidersprüche fort. Während bei dem Versand einer E-Mail zukünftig Verbindungsdaten des Übertragungsvorgangs für die Dauer der gesetzlichen Mindestspeicherungsfristen gespeichert werden, wird bei der Versendung von Briefen keine Erfassung der Versandvorgänge vorgenommen.

Aktuelle Diskussion um die Vorratsdatenspeicherung

Der Gesetzesentwurf zur Einführung einer Vorratsdatenspeicherungspflicht beruhte auf einer EU-Richtlinie aus dem Jahr 2006. Vorausgegangen sind zahlreiche erfolglose Gesetzesinitiativen zur Einführung einer Verpflichtung der Internetprovider zur verdachtsunabhängigen Speicherung von Verbindungsdaten in Deutschland. Daß nunmehr über den Umweg europäischer Vorgaben eine Vorratsdatenspeicherung in Deutschland eingeführt werden soll, die im nationalen Parlament nie eine Mehrheit fand, ist zwar auf den ersten Blick paradox – grundsätzliche Bedenken gegen europäische Vorgaben bestehen aber nicht. Gleichwohl hat das gewählte Verfahren zur Einreichung zweier Klagen gegen die Richtlinie geführt. Das Verfahren auf europäischer Ebene ist aus zwei

Gründen bemerkenswert. Zum einen stellt die Einführung der Vorratsdatenspeicherung insoweit einen Paradigmenwechsel dar, als die Internetprovider bislang aufgrund von EU-Vorgaben verpflichtet sind, alle Daten, die für die Abrechnung der in Anspruch genommenen Dienste nicht von Bedeutung sind, nach Beendigung der Nutzung des Dienstes zu löschen. Zum anderen verwundert die für EU-Verhältnisse erstaunlich kurze Zeit von weniger als fünf Monaten zwischen der Annahme des Vorschlags der Richtlinie und der Annahme durch den Rat der Europäischen Union. Berücksichtigt man den Umstand, daß mehrjährige Beratungen von Rahmenbeschlüssen oft mit der Notwendigkeit intensiver Beratung gerechtfertigt werden, erscheint fraglich, ob die intensive Kritik am Richtlinienentwurf in der kurzen Zeit ausreichend geprüft wurde.

Vorgaben der Richtlinie und Kritik

Die Richtlinie verpflichtet die Mitgliedstaaten unter Bezugnahme auf die Terrorismusbekämpfung, die gesetzlichen Rahmenbedingungen für eine europaweit harmonisierte Vorratsdatenspeicherung zu schaffen. Dies bedeutet insbesondere, daß die Mitgliedstaaten verpflichtet sind, die Vorratsspeicherung der in Art. 5 der Richtlinie genannten (Verbindungs-)Daten, die während der Kommunikation anfallen, als gesetzliche Verpflichtung der Diensteanbieter zu verankern. Die Verpflichtung der Richtlinie ist sowohl aufgrund der leichten Umgehungsmöglichkeiten, als auch aufgrund rechtlicher Bedenken gegen die Zulässigkeit einer entsprechenden Verpflichtung auf Kritik gestoßen.

Die Kritik an der leichten Umgehungsmöglichkeit, die Fragen nach der Effektivität der Maßnahme aufwirft, wendet sich gegen das Hauptargument der Befürworter einer Vorratsdatenspeicherung. Diese stützten sich darauf, daß durch die vollständige Speicherung von Verbindungsdaten verhindert werden könnte, daß einzelne Kommunikationsvorgänge unerkannt blieben. Angesichts der Möglichkeiten, durch den Einsatz von Anonymisierungsdiensten oder Proxyservern aus Ländern ohne Vorratsdatenspeicherungspflicht die Zuweisung der Daten zu umgehen, erscheint dies allerdings fraglich. Auch führen die Verbindungsdaten nicht notwendig unmittelbar zum Verdächtigen, sondern erlauben zunächst nur die Identifikation des genutzten Anschlusses oder der verwendeten E-Mail-Adresse. Hat der Verdächtige öffentliche Hot-Spots und ohne Registrierung erhältliche E-Mail-Adressen genutzt, so endet trotz Vorratsdatenspeicherung die Spur zum Verdächtigen regelmäßig vor dessen Identifikation.

Berücksichtigt man weiter, daß sich der Zugang zu solchen Diensten einfach gestaltet, so muß davon ausgegangen werden, daß auch im Zusammenhang mit kriminellen und insbesondere terroristischen Aktivitäten auf diese Dienste zurückgegriffen wird, was die Vorratsdatenspeicherung insoweit leerlaufen läßt. Verhindern ließe sich dies nur durch eine erhebliche Ausweitung von Maßnahmen zur Einschränkung anonymer Kommunikation, wie beispielsweise der Verpflichtung zur Identifikation von Nutzern öffentlicher Internetzugänge, die beispielsweise in Italien besteht. In rechtlicher Hinsicht berühren die Bedenken der Kritiker unterschiedliche Aspekte. Im Vordergrund stehen dabei verfassungsrechtliche Bedenken. Während die Begründung der Richtlinie darauf verweist, daß die Einführung der Vorratsdatenspeicherung eine unverzichtbare Maßnahme darstelle, sehen die Kritiker einen Eingriff, der insoweit verfassungsrechtlich bedenklich erscheint, weil alternative, weniger intensive Ermittlungsinstrumente zur Verfügung stehen.

Alternative Ermittlungsinstrumente

Vor dem Hintergrund der verfassungsrechtlichen Bedenken, die sich maßgeblich auf die Verfügbarkeit alternativer, weniger eingriffsintensiver Ermittlungsansätze konzentriert, kommt der Suche nach Alternativen zur Vorratsdatenspeicherung eine zentrale Bedeutung zu. Ein solcher alternativer Ansatz findet sich in Art. 16 der Cybercrime Convention des Europarates. Die Konvention, die 2001 zur Unterzeichnung ausgelegt und bislang von 43 Staaten unterzeichnet wurde, ist anders als die Vorratsdatenspeichung kein regionaler (EU-)Ansatz, sondern der bislang einzige globale Ansatz

zur Harmonisierung der bisweilen sehr unterschiedlichen nationalen Ansätze zur Bekämpfung der Internetkriminalität. Die Konvention ist auch für Nichtmitglieder des Europarates offen und wurde unter anderem von Kanada, Japan und den USA unterzeichnet. Art. 16 der Cybercrime Convention verpflichtet die Unterzeichner, eine auch als „Quick Freeze" bezeichnete beschleunigte Sicherung der Daten vor einer Löschung im Verdachtsfall einzuführen.

Anders als bei der Vorratsdatenspeicherung, bei der ohne Selektion sämtliche Verbindungsdaten gespeichert werden, werden bei der Maßnahme gemäß Art. 16 nur die Daten vor einer Löschung bewahrt, die für die Ermittlungen von Bedeutung sind. Vergleicht man die Vorratsdatenspeicherung mit der „Quick Freeze"-Anordnung, so ergeben sich zwei Unterschiede. Die „Quick Freeze"-Anordnung läuft in den Fällen ins Leere, in denen zum Zeitpunkt des Erlasses der Anordnung die relevanten Daten bereits gelöscht wurden. Insoweit erscheint die „Quick Freeze"-Anordnung auf den ersten Blick keine ernsthafte Alternative zur Vorratsdatenspeicherung zu sein. Die Unterschiede relativieren sich jedoch erheblich, wenn man zum einen berücksichtigt, daß bei den großen Zugangsprovidern bis zur Löschung der Verbindungsdaten regelmäßig mehrere Tage vergehen und zum anderen nicht außer acht läßt, daß auch die Konsequenzen der Vorratsdatenspeicherung technisch umgangen werden können.

Ausblick

Die Diskussion um die Notwendigkeit und rechtliche Zulässigkeit der Vorratsdatenspeicherung ist mit der Annahme des EU-Rahmenbeschlusses keinesfalls abgeschlossen. Berücksichtigt man die oben dargestellten Bedenken, so erscheint sowohl die Notwendigkeit als auch die rechtliche Zulässigkeit fraglich. Im Rahmen der weiteren Diskussion wird dem Umstand, daß sich der Europarat im Zusammenhang mit der Cybercrime Convention gegen eine Vorratsdatenspeicherung entschieden hat, eine besondere Bedeutung zukommen.

Trotz der Bedeutung der Auseinandersetzung mit der Vorratsdatenspeicherung sollten in der Diskussion die übrigen Entwicklungen im Bereich der Schaffung neuer Ermittlungsinstrumente – wie beispielsweise die Online-Durchsuchung – nicht aus den Augen verloren werden. Dies gilt selbstverständlich auch für die übrigen Bestrebungen zur Regulierung des Internet und zur Effektivierung der Strafverfolgung, wie etwa die immer wieder aufflammenden Diskussionen um eine Regulierung von Kryptographie- und Anonymisierungstechniken. Legislative Ansätze wie beispielsweise das in Italien eingeführte Verbot der anonymen Nutzung von öffentlichen Internetterminals werden sowohl auf nationaler als auch auf internationaler Ebene sorgsam beobachtet.

[1] *http://www.bundesverfassungsgericht.de/entscheidungen/rk20070511_2bvr054306.html*

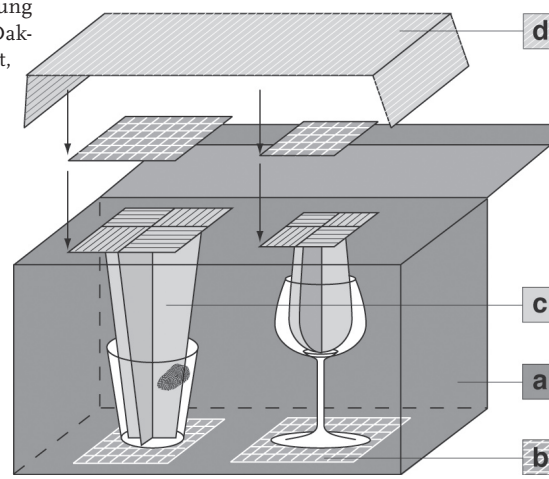
Basteltips Biometrieversand

von evelyn und starbug

Auf der folgenden Seite haben wir euch euer persönliches Problempolitiker-Sammelalbum mitgeliefert. Den ersten Abdruck gibt es in diesem Heft. Um allen anderen Lesern dabei zu helfen, ihre Sammlung zu vervollständigen, ist nun eure Mithilfe gefragt.

Eine gute Gelegenheit, an die Fingerabdrükke unserer demokratischen Vertreter zu kommen, bieten Latenzabdrücke auf Gläsern und Flaschen. Nur sind diese Fettrückstände leider sehr empfindlich. Schon beim Anheben müßt ihr aufpassen, keine eigenen Abdrücke zu hinterlassen, wollt ihr nicht versehentlich mit einem Politiker verwechselt werden. Am sichersten ist, wenn ihr beherzt mit drei oder mehr Fingern von innen zupackt und auf die Reibung vertraut. Wenn ihr dann nicht selber den Daktyloskopen eures Vertrauens aufsuchen wollt, müßt ihr das Glas den treuen Händen eines Logistikdienstleisters anvertrauen. Da aber schon leichte Berührungen mit der Paketwand die Abdrücke unwiederbringlich zerstören können, scheidet das Einwickeln in Papier oder Schaumstoff aus.

Daher möchten wir euch hier das Bastelset für eine Versandbox zum sicheren Transport von Gläsern mit Fingerabdrücken vorstellen.



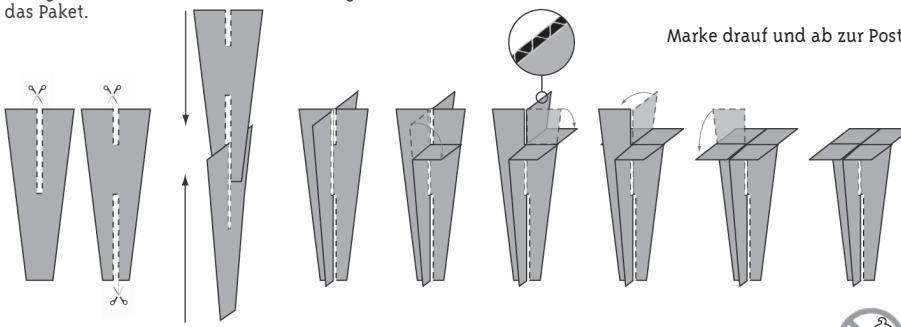
a Wir suchen uns einen Karton der Größe des zu transportierenden Glases.

b Wir plazieren einen Streifen doppelseitigen Teppichklebebands in der Mitte des Kartons, stellen vorsichtig das Glas drauf und drücken es leicht fest.

c Ist das Glas am Boden fixiert, bauen wir die Deckelhalterung. Länge und Breite des Einsatzes orientieren sich dabei an der Form des Glases (siehe unten).

d Schließlich kleben wir auch auf die obere Pfalz des Einsatzes einen Streifen des Klebebands, befestigen daran den Einlegedeckel und verschließen vorsichtig das Paket.

c



Marke drauf und ab zur Post!

Das biometrische Sammelalbum

Deutsche Edition 2008

Wolfgang Schäuble
Bundesinnenminister

Angela Merkel
Bundeskanzlerin

Günther Beckstein
Ministerpräsident Bayern

Moritz Harms
Bundesanwältin

Otto Schily
Ex-Innenminister

Jörg Ziercke
BKA-Präsident

La Zypries

Wolfgang "No Privacy" Schäuble

Günther "präventiv wegsperren" Beckstein

"auf Augenhöhe mit Terroristen": The Harms

Jörg "Wir brauchen alles" Ziercke

Er öffnet nie seine eMails – und doch ist er…

"Großes, völlig absurdes Kino"

"Nie wurden Ihre Grundrechte so verletzt…"

Der Bundestrojaner

Demnächst in Ihrem Computer