Digitaler Tsunami

Pünktlich zum 11.09. meldet die c't: „EU-Innenpolitiker rüsten sich für den „digitalen Tsunami – (…) Das Papier führt weiter aus, dass die bargeldlosen Einkäufe bereits durchsuchbare Echtzeitinformationen erzeugen. Dieser Trend werde durch den zunehmenden Einsatz biometrischer Identifizierungsmaßnahmen sowie von Kameras zur Videoüberwachung verstärkt. Das Online-Verhalten der Nutzer würde den digitalen Tsunami noch weiter vergrößern. Vor allem soziale Netzwerke und virtuelle Welten – aber letztlich alle Formen von Aktivitäten im Internet – „generieren gewaltige Informationsmengen, die für öffentliche Sicherheitsorganisationen nützlich sein können". Am Ende der Entwicklung stünden lebenslange Datenbanken über Individuen. Auf technische Möglichkeiten zur Sicherung der Privatsphäre geht das Konzept zwar kurz ein; allerdings nur unter dem Aspekt, dass diese auch von „Terroristen und anderen Kriminellen" genutzt werden könnten. Anonymisierungsdienste, Verschlüsselungswerkzeuge sowie sogar Instrumente zum automatischen Löschen von Browser-Cookies haben so einen unangenehmen Beigeschmack für die Verfasser des portugiesischen Papiers, da sie helfen könnten, Verbrechenspläne zu verbergen und die Polizei bei ihrem Bemühungen zur Informationssammlung zu behindern. (…) Für Tony Bunyan von Statewatch ist damit klar, dass mit dem Stockholmer Programm die EU endgültig in einen Überwachungsstaat verwandelt werden soll und sich in Richtung eines autoritären Staatengebildes bewegt. (…)"

Online-Durchsuchung, revisited

Die Stellungsnahmen der Sachverständigen zur so genannten „Online-Durchsuchung“:
Prof. Dr. Christoph Gusy, Universität Bielefeld – Ausschussdrucksache 16(4)460 A
Dr. Fredrik Roggan, Rechtsanwalt, Berlin – Ausschussdrucksache 16(4)460 B
Prof. Dr. jur. Dirk Heckmann, Universität Passau – Ausschussdrucksache 16(4)460 C
Prof. Dr. Martin Kutscha, Fachhochschule für Verwaltung und Rechtspflege, Berlin – Ausschussdrucksache 16(4)460 D
Peter Schaar, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit , Bonn – Ausschussdrucksache 16(4)460 E
Peter Dathe, Präsident des Bayerischen Landeskriminalamtes, München – Ausschussdrucksache 16(4)460 F
Jörg Ziercke, Präsident des Bundeskriminalamtes, Wiesbaden – Ausschussdrucksache 16(4)460 G
Prof. Dr. Hansjörg Geiger, Staatssekretär a.D., Berlin – Ausschussdrucksache 16(4)460 H
Prof. Dr. Markus Möstl, Universität Bayreuth – Ausschussdrucksache 16(4)460 I
Prof. Dr. Ralf Poscher, Ruhr-Universität Bochum – Ausschussdrucksache 16(4)460 J

Ich frage mich, wieso die keinen IT-Experten geladen haben? Ich werde die Gutachten studieren unter dem besonderen Aspekt, womit die Herren begründen, dass so etwas technisch machbar sei.

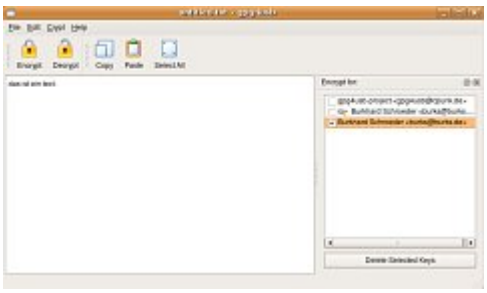
„Datenschutz contra Opferschutz“

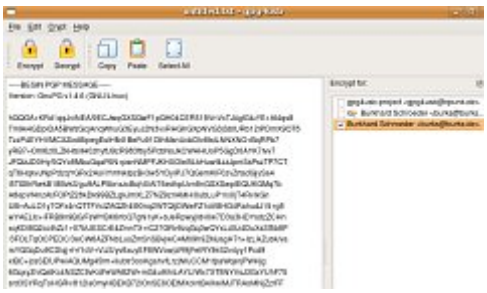
Tendenziöse Meinungsmache bei report München: „Datenschutz contra Opferschutz“. Dazu netzpolitik.org: „report München mit Falschinformationen gegen Datenschutz“ – „Fazit: Schlecht recherchierte, plumpe Meinungsmache.“ Heise: „Datenschützer werfen Report München Meinungsmache für Vorratsdatenspeicherung vor“.
By the way: Der Autor des Beitrags, Oliver Bendixen, ist Polizeireporter beim bayerischen Rundfunk. Vermutlich ist er vorher „einschlägig“ gebrieft worden – wie schon in anderen Fällen. Wozu braucht die Polizei noch eine Pressestelle, wenn es solche Journalisten gibt?

---

gpg4usb

Ich empfehle allen Windows- und Linux-Usern ein kleines Programm: gpg4usb. „gpg4usb ist ein neues, portables Programm zur Verschlüsselung von Texten. Die Vorteile dieser noch sehr jungen Software liegen auf der Hand: gpg4usb ist schnell und einfach auf einem usb-Stick zu installieren, und noch dazu lauffähig unter Windows und Linux (…). Es handelt sich dabei um einen einfachen Texteditor, verbunden mit einem GnuPG-Frontend zur Verschlüsselung. Mit diesem Tool sollte es nun ein Leichtes sein, bei Freunden, auf der Arbeit oder in Internet-Cafes Nachrichten sicher zu versenden. Auf dem jeweiligen Rechner wird nichts installiert, und es werden keine installierten Programme vorausgesetzt.“ [via cpunk – the cypherblog.de]





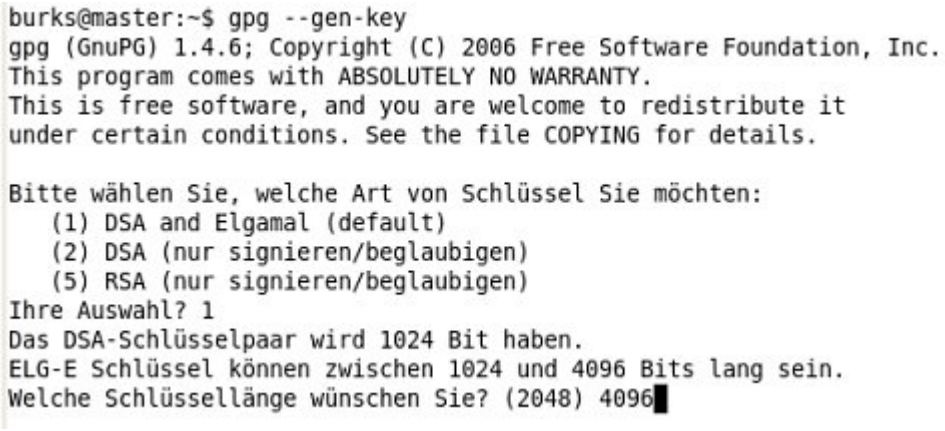
Kann ich bestätigen, obwohl ich zunächst die Linux-Version nicht gefunden habe. Die Lösung: *Beide* Versionen – Linux und Windows – sind in demselben zip-File enthalten. Nach dem Entpacken kopiert man das Verzeichnis irgendwohin und startet mit start_linux (oder klickt auf die Windows-exe). Dann die Schlüssel importieren, die man gerade benutzen muss. Der Rest ist selbsterklärend. Das war's schon. Sehr praktisch.

Provider OVH mag keine TOR-Exit-Nodes

Gulli:news: Der Hosting-Provider OVH schaltete die Server der German Privacy Foundation (GPF) und der Humanistischen Union (HU) sowie weiterer Organisationen und Einzelpersonen unter möglicherweise vorgeschobenen Gründen ab. Die German Privacy Foundation e. V. betreibt derzeit drei leistungsfähige TOR-Nodes, zwei Mixmaster Remailer und einen I2P-Knoten. Mitglieder des Vereins betreiben weitere Server in eigener Verantwortung mit Unterstützung der GPF e. V. Ein weiterer der vereinseigenen TOR-Server wurde nun mit wechselnden Begründungen abgeschaltet; das bisher bezahlte Geld will der Provider behalten." [mehr…]

Nur *ein* Server von uns wurde abgeschaltet, die anderen drei (gpfTOR1-3) sind bei anderen Providern angemeldet.

Neuer Schlüssel



Ich habe heute einen neuen Schlüssel für die E-Mail-Adresse burks@burks.de erzeugt – bitte importieren! (Der alte Schlüssel war am 10.08. abgelaufen).
ID:01B66647C23A7B46 | Fingerprint: 1EE1 D41C 0AC8 FEF9 AE08 DA1C 01B6 6647 C23A 7B46

Tunnel aus Burma

Ich frage mich, welcher Sinn und welche pädagogisch wertvolle Botschaft sich hinter Artikeln verbergen, die sich mit der Zensur des Internet in anderen Ländern verbergen? Sollen sich die Rezipienten nur gruseln? Soll sie ein lähmendes Gefühl beschleichen; wie pöhse die Zensoren sind? Artikel wie in Spiegel „online“ über die Zensur in Burma sind sinnlos, wenn die Leserinnen und Leser nichts daraus lernen, zum Beispiel wie man Zensur umgeht. „Ein paar Handgriffe nur, eine Tunnel-Software wird aktiviert, ein Proxyserver in den USA angewählt, schon ist das Regime ausgetrickst.“ Versteht das jemand? Wenn

es so einfach wäre mit der „Tunnel-Software„, warum fehlt das in den Berichten über China?

Wenn Spiegel „online“ die Leser ernst nähme, Online-Journalismus betriebe und nicht nur auf sich selbst verlinkte, wäre zum Beispiel ein Link auf den entsprechenden Wikipedia-Artikel hilfreich, damit man sich darauf vorbereiten kann, wenn Schäuble und Genossen das hierzulande verwirklichen, wovon sie träumen. (Ja, der Satz ist zu lang, aber ich sitze in einem Ferienhaus in Jütland und will nicht allzu lange nachdenken, weil ich nur noch einen Tag Urlaub habe.)

Nur zur Erinnerung eine der zahlreichen Falschmeldungen zur so genannten „Online-Durchsuchung“, hier der Tagesspiegel: „Das Bundeskriminalamt (BKA) soll künftig mittels einer neuen Software die Daten von privaten Rechnern ausspionieren können. Das bestätigte das Bundesinnenministerium (BMI) dem Tagesspiegel auf Anfrage. Das System der sogenannten ‚Online-Durchsuchung‘ sei bereits in diesem Jahr mehrfach angewandt worden und sei Teil des 132 Millionen Euro schweren Sonderprogramms zur Stärkung der inneren Sicherheit. Die Ermittler sollen sich dabei auf richterliche Anordnung unbemerkt via Internet in die Computer von Privatpersonen einloggen können, gegen die ein Strafverfahren läuft.“ Zum Glück war das fast alles gelogen: Die „Online-Durchsuchung“ war mitnichten angewandt worden und ist auch nicht Teil des PSIS (Z5-007 300/120 (10.10.2006).

Wo ist der qualitative Unterschied zur Praxis in Burma? „Alle fünf Minuten müsste der Inhaber eines Internet-Cafés einen Screenshot all seiner Computer erstellen: ein Foto aller Seiten, die gerade geöffnet sind. Er müsste das alles speichern.“ Das ist noch nicht einmal so schlimm wie eine Spionagesoftware, die der Staat direkt auf den Rechnern von mehr oder minder Verdächtigen installiert. In Burma sind alle verdächtig, in Deutschland (noch) nicht. Aber was nicht ist, kann ja noch werden.

Hansetrojaner

Mit Schmunzeln habe ich bei Heise „Hamburgs Innensenator plant den Hansetrojaner“ gelesen. Die hübsche Story geht auf die taz zurück. „Online-Razzien seien heute ein ‚unverzichtbares Instrument‘ der Strafverfolger“, sagt Hamburgs Innensenator Christoph Ahlhaus. Ahlhaus ist ein Lügner, denn ein Instrument ist dann nicht „unverzichtbar“, wenn es gar nicht funktioniert und wenn es noch nie erfolgreich angewendet wurde. Der gute Mann ist gelernter Bankkaufmann und Jurist und hat vom Internet und von Computern so viel Ahnung wie ein Zeuge Jehovas vom Atheismus. Ich überlege, ob wir ihm Ende des Monats mal ein Büchlein schicken. Aber solche Leute sind meist so eingebildet, dass sie aufs Lesen und Erwägen rationaler Argumente gern verzichten. „Weitere Einzelheiten zu dem Vorhaben sind bislang nicht bekannt“, schreibt Krempl bei heise.de. Quod erat demonstrandum. Wie auch. Es gibt keine.

Alle bespitzeln alle

FTD.de: “ Der Kölner Konzern Gerling hat Telefon- und E-Mail-Zieldaten eigener Mitarbeiter ausspioniert. Ziel war es, eine undichte Stelle in dem Versicherungskonzern zu finden.“ Will sagen: Die Mitarbeiter des Konzern schrieben nur elektronische Postkarten und verhielten sich wenig sicherheitsbewusst. „Im konkreten Fall ging es nach FTD-Informationen um einen Bericht im Magazin „Capital„, der im Februar 2004 erschien und sich mit den gekürzten Betriebsrenten bei Gerling beschäftigte.“ [Bericht der Capital]

Ohne Worte | Speicherwahn im Kabinett

Sueddeutsche.de (02.07.): „Justizministerin Zypries und der oberste Datenschützer Schaar diskutierten in Berlin das neue ‚Computergrundrecht'. (…) Die Referenten, mehrheitlich Juristen, gaben offen zu, dass sie keine Ahnung von Technik haben. Selbst der Spruch ‚Um Computer und Internet kümmert sich meine Frau' fiel: Im Hause des innenpolitischen Sprechers der SPD, Dieter Wiefelspütz, darf die Gattin den Rechner wieder hochfahren, wenn er abgestürzt ist." Man fasst es nicht…

Die nächste Klage gegen die „Online-Durchsuchung"

…ist vorprogrammiert. Heise.de meldet über „Bayerischer Landtag setzt den „Bayerntrojaner" frei": „Im Rahmen einer Online-Razzia sollen die Sicherheitsbehörden auch Daten etwa auf Festplatten löschen oder verändern dürfen, wenn Gefahr für höchste Rechtsgüter besteht. Den Fahndern wird zudem erlaubt, für die Installation von Spähprogrammen auf Zielrechner in die Wohnungen Betroffener einzudringen und diese dabei auch zu durchsuchen." Bei veränderten Daten haben die Ergebnisse sowieso keinen forensischen Wert mehr. Das ist doch sowohl grober Unfug als auch Volksverdummung. Ich frage mich, ob die in Bayern das Urteil des Bundesverfassungsgerichts vom

27.2.2008 überhaupt jemals gelesen oder gar verstanden haben. Die höchsten Richter werden die real gar nicht existierende bayerische „Remote Forensic Software“ in kleine Stücke zerlegen und Beckstein um den Hals wickeln…

Honeytrap | Unsichere Software

Der Vorstand der German Privacy Foundation bekam kürzlich interessante Post, die ich hier auszugsweise wiedergebe:

“ (…) Am (…) richtete ich auf Ihrer Seite https://privacybox.de/ einen Account in der *PrivacyBox* ein. Unter einem Pseudonym wollte ich auch für Menschen anonym erreichbar sein, welche die in Deutschland m. E. exzessiv ausufernde Staatsschnüffelei nicht für richtig halten.

Bei einem Testlauf startete ich die personalisierte Seite (https://privacybox.de/persoehnlich.msg) aus einem älteren Microsoft Outlook Express Adressbuch (*.wab) heraus, woraufhin der Browser (Firefox 3.0) auf (http://www.theedge.com/) umgeleitet wurde, wo der Fragebogen offensichtlich dem verblüfften User auf die ganz dumme Art Kontaktdaten herauslocken soll. Diesen Server habe ich in Texas, USA, lokalisiert (…). Das Verhalten ist reproduzierbar und geschieht nur bei dieser Webseite, andere werden anstandslos angesteuert. Auch der POP3-Abruf per E-Mail-Programm funktioniert.

Wurde bzw. wird Ihr Dienst, Ihr Server bzw. Ihr Hoster oder auch „nur“ Ihre Seite u. U. von US-Sicherheits-Diensten oder Diensten i. V. m. diesen im Zuge der weltweiten „Terroristenfahndung“ gehackt und missbraucht? Oder ist die

Umleitung auf die offensichtlich in den USA gehostete Seite (siehe Anhang!) http://www.theedge.com/ von PrivacyBox und/oder Ihrem Hoster so gewollt?

(…) Die zweite Möglichkeit, dass die gesamte „PrivacyBox“ eine Art von „Honeytrap“ der international zusammenarbeitenden Sicherheitsbehörden ist, in welcher quasi wie in einer „Sandbox“ im Sandkasten – unter Aufsicht der „Erwachsenen“ – die Unmündigen ihre dummen Geheimnisse austauschen können, mag ich nicht nur nicht ausschließen, sondern das liegt nach meinen Erfahrungen mit ihren Methoden und dieser Seite direkt nahe. (…)“

Ein Vorstandsmitglied hat geantwortet:

“ (…) danke für den Hinweis. (…) Ich habe das Phänomen gerade selbst getestet und komme mit Outlook Express zum selben Ergebnis. Das liegt aber nicht an der PrivacyBox, sondern es ist ein Fehler in Outlook Express, das die URL immer mit einem http:// voran an Firefox übergibt. Sie können die Sache direkt selbst mit beliebigen https-URLs in Firefox testen:

http://https://privacybox.de -> landet bei theedge.com
http://https://www.postbank.de -> ebenfalls

(…) Ich kann versichern, daß die Privacy Foundation die beobachtete Umleitung nicht beabsichtigt hat. Die Box ist kein Honeypot und späht keine Daten im Interesse irgendwelcher Dienste aus. Wir empfehlen Ihnen, veraltete und unsichere Software wie Outlook Express zu meiden.“

PrivacyBox | Tarnkappe für E-Mails

Wir hatten ein relativ gutes Presseecho über die PrivacyBox. Heute berichtet die taz: „Nachrichten übers Internet anonym zu verschicken, ist mit herkömmlichen Mailprogrammen praktisch nicht möglich. Die „PrivacyBox“ soll helfen.“

Aber: Der Sinn der PrivacyBox ist weniger die Anonymität, sondern dass die Vorratsdatenspeicherung unterlaufen werden könnte, falls sie in Kraft träte (nach der gegenwärtigen Gesetzeslage am 01.01.2009). Über Anonymität, auch bei E-Mails, könnte sich jeder informieren – das überfordert den DAU nicht. Man muss nur wollen. Daran hapert es aber, vor allem bei Journalisten.

By the way: „Vorige Woche hatte die „German Privacy Foundation“ den neuen Service im Büro des Datenschutzbeauftragten der Bundesregierung, Alexander Dix, vorgestellt.“ Auch falsch. Dix ist der Berliner Beauftragter für Datenschutz und Informationsfreiheit. Grmpf.

EuGH: Verhandlung über Klage gegen VDS am 1. Juli

Virtuelles Datenschutzbüro: „Der Europäische Gerichtshof (EuGH) hat die mündliche Verhandlung über die Beschwerde Irlands und der Slowakei gegen die Richtlinie zur Vorratsdatenspeicherung (VDS) für den 1. Juli angesetzt.“

„Die Klage richtete sich nicht gegen den Inhalt der

Richtlinie, sondern gegen ihre Form: Eine Richtlinie sei die falsche Rechtsgrundlage, so die irische Klage, die angemessene Form sei ein Rahmenbeschluss. Richtlinien sind ein Instrument der ‚ersten Säule' der EU, die hauptsächlich für den Binnenmarkt zuständig ist, Rahmenbeschlüsse sind ein Mittel der ‚dritten Säule', die für die Zusammenarbeit von Polizei und Justiz zuständig ist. Rahmenbeschlüsse werden im Rat der Europäischen Union einstimmig beschlossen, während Richtlinien im Mitentscheidungsverfahren mit der Kommission und dem Europäischen Parlament dort nur eine qualifizierte Mehrheit benötigen. Bestrebungen, eine Vorratsdatenspeicherung mittels eines Rahmenbeschlusses einzuführen, waren gescheitert, da der notwendige Konsens nicht zu erreichen war. Vor diesem Hintergrund wurde die Rechtsgrundlage gewechselt; die Richtlinie wird in ihrer Begründung in erster Linie als Mittel der Marktharmonisierung für Telekommunikationsunternehmen dargestellt.

Sollte die Richtlinie fallen, wovon viele Beobachter ausgehen, wäre der Weg frei für das Bundesverfassungsgericht (BVerfG), das deutsche Umsetzungsgesetz zur Vorratsdatenspeicherung zu kippen. Das BVerfG übt gemäß seinem ‚Solange-II'-Beschluss seine Normemkontrollkompetenz gegenüber Umsetzungen von EU-Recht zur Zeit nicht aus; es geht davon aus, dass europäische Rechtsakte im Allgemeinen einen mit den hiesigen Standards vergleichbaren Grundrechtsschutz gewährleisten und verzichtet daher auf die Kontrolle, die der Europäische Gerichtshof übernehmen kann. Wenn die Richtlinie gekippt wird, verlieren die sie umsetzenden Regelungen in der Strafprozessordnung und dem Telekommunikationsgesetz ihren Status als Umsetzung von EU-Recht und könnten ganz normal verhandelt werden."

Privacybox für Whistleblower und Journalisten vorgestellt

Heise.de: „Die German Privacy Foundation hat im Büro des Berliner Datenschutzbeauftragten Alexander Dix die PrivacyBox vorgestellt. Die mit Open-Source-Software programmierte Box ist ein mit jedem Browser zu erreichendes Web-Formular, das Journalisten, Bloggern sowie ihren Informanten und Hinweisgebern („Whistleblower“) eine anonyme und vorratsdatenfreie Kontaktmöglichkeit anbietet.“ [mehr]

PrivacyBox, reloaded

Wer eine verschlüsselte und anonyme (!) E-Mail an mich schreiben will, kann das jetzt auch tun über die PrivacyBox: https://privacybox.de/burks.msg (bitte Absender angeben, wenn ich antworten soll).

PrivacyBox

Presseportal.de (ots): „German Privacy Foundation stellt die PrivacyBox vor – eine anonyme Kontaktmöglichkeit für Informanten“

Berlin (ots) – Die German Privacy Foundation hat am 09.06.2007 auf eine Pressekonferenz in Kooperation mit dem Berliner Datenschutzbeauftragten die PrivacyBox vorgestellt. Mit diesem

Web-Interface können potenzielle Informanten anonym und verschlüsselt Nachrichten an Journalisten versenden.

Der aktuelle Skandal um Datenspionage bei der Telekom, aber auch die Diskussion um die Vorratsdatenspeicherung haben gezeigt, dass Journalisten die Möglichkeit haben müssen, ihre Informanten zu kontaktieren, ohne dass jemand protokollieren kann, wer mit wem kommuniziert hat. Genau das leistet die PrivacyBox. Technische Vorkenntnisse sind nicht erforderlich – weder beim Empfänger noch beim Sender. Der Programmcode ist quelloffen („Open Source“), kostenlos und steht auf Nachfrage auch anderen Interessierten offen.

Dr. Alexander Dix, der Berliner Beauftragte für Datenschutz und Informationsfreiheit, wünschte sich, dass viele Bürgerinnen und Bürger eine derartige Möglichkeit nützten, sicher und anonym zu kommunizieren.

Burkhard Schröder, Journalist und Vorstandsvorsitzender der German Privacy Foundation, erklärte, ab jetzt sei es nicht mehr möglich, einen Whistleblower oder Informanten der Medien zu identifizieren, auch wenn dessen Unternehmen versuche, ihn auszuspionieren: „Die PrivacyBox stärkt die Pressefreiheit und den Pressegeheimnisschutz.“ Der Informatiker Karsten Neß, Mit-Entwickler der PrivacyBox, kündigte an, dass man ab 2009 zwar gesetzlich verpflichtet sei, die Rechner-Adressen der Nutzer der PrivacyBox zu speichern, dass es jedoch möglich sei, auch diese IP-Adresse zu anonymisieren. Die Entwicklung der PrivacyBox wurde unter anderem durch eine Spende des Deutschen Fachjournalisten-Verbandes unterstützt.

Der im Oktober 2007 gegründete gemeinnützige Verein German Privacy Foundation e.V. informiert über sichere Kommunikation im Internet und organisiert und unterstützt Weiterbildungs- und Aufklärungmaßnahmen für Erwachsene und Jugendliche. Die Mitglieder des Vorstands und die Mitglieder verpflichten sich, über Vereinsangelegenheiten ausschließlich verschlüsselt zu kommunzieren. Die German Privacy Foundation will erreichen,

dass das Thema „Sicherheit im Internet“ besser und sachgerechter in den Medien dargestellt wird.

Pressekontakt:

www.privacyfoundation.de/
info@privacyfoundation.de
https://privacybox.de
Burkhard Schröder 0172 3829895

Vgl. auch:
N-TV: „Mit der „Geheimkiste“ Lauscher austricksen“
golem.de: „Verschlüsseltes Kontaktsystem für Journalisten“

PrivacyBox

German Privacy Foundation e.V.
10965 Berlin
www.privacyfoundation.de/
info@privacyfoundation.de

Einladung zur Pressekonferenz der German Privacy Foundation in Kooperation mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit:
am Montag, 09.06.2008, 10.30 Uhr
Berliner Beauftragter für Datenschutz und Informationsfreiheit
An der Urania 4-10
10787 Berlin
www.datenschutz-berlin.de
Tel. 49.30.13889-0
9. Etage

Die PrivacyBox- anonyme Kontaktmöglichkeit für Informanten

Sehr geehrte Damen und Herren,

liebe Kolleginnen und Kollegen,

Die German Privacy Foundation hat eine Software entwickelt, mit der potenzielle Informanten anonym und verschlüsselt Nachrichten an Journalisten versenden können. Das geschieht über ein Web-Interface. Das Programm ist quelloffen („Open Source“), kostenlos und steht auf Nachfrage auch anderen Interessierten offen.

Der aktuelle Skandal um Datenspionage bei der Telekom, aber auch die kontroverse Diskussion um die Vorratsdatenspeicherung haben gezeigt, dass Journalisten die Möglichkeit haben müssen, ihre Informanten zu kontaktieren, ohne dass jemand protokollieren kann, wer mit wem kommuniziert hat. Genau das leistet die PrivacyBox. Technische Vorkenntnisse sind nicht erforderlich – weder beim Empfänger noch beim Sender.

Wir würden Ihnen gern die PrivacyBox vorstellen und Ihre Fragen beantworten. Als Gesprächspartner werden Ihnen zur Verfügung stehen: Dr. Alexander Dix, Berliner Beauftragter für Datenschutz und Informationsfreiheit, Burkhard Schröder, Vorsitzender der German Privacy Foundation, Karsten Ness, Informatiker, für das Entwickler-Team der GPF, Kai Biermann, ZEIT online.

Mit freundlichen Grüßen
Burkhard Schröder

Understanding individual human mobility patterns

Nature: „Understanding individual human mobility patterns“, vgl. auch heise.de: „Wissenschaftler analysieren individuelle

Bewegungsprofile von Handynutzern“: „Die Bewegungsmuster der einzelnen Menschen haben die Wissenschaftler in räumliche Wahrscheinlichkeitsverteilungen zusammenfassen können, nach denen deutlich werde, dass Menschen trotz ihrer unterschiedlichen Bewegungen ‚einfachen, sich wiederholenden Mustern‘ folgen.“ Für das Denken gilt das vermutlich auch….

„Der Zweck des Staates ist die Wahrung der Freiheit“

Dokumentation: Hans-Jürgen Papier, Präsident des Bundesverfassungsgerichts: „Über das Spannungsverhältnis von Freiheit und Sicherheit aus verfassungsrechtlicher Sicht“ – Ein Vortrag auf der Tagung „Freiheit und Sicherheit – Verfassungspolitische Dimensionen“ der Akademie für Politische Bildung Tutzing am 30. Mai 2008.