Die BigBrotherAwards 2011

BigBrotherAwards 2011 – wenn man sich die Details ansieht, verschlägt es einem glatt die Sprache ob der Dreistigkeit einiger Firmen, Organisationen und Politiker.

Facebook: „Generationenübergreifende Datenerfassung auf freiwilliger Basis unter der Maske der Freundschaft? Ich habe Angst.“ – Zensuskommission: „Mit dem Zensus 2011 werden riesige Mengen von Daten gesammelt, welche es erlauben, Personengruppen zu selektieren. Für die Sonderbehandlung der Juden im ‚3. Reich‘ war das die Grundlage für die spätere Vernichtung.“

Vorratsdatenspeicherung in Frankreich

Netzpolitik.org: „Neben den bereits bekannten und in der Richtlinie genannten Daten wie IP-Adressen, Telefonnummern, Email-Adressen(…) ist in letzter Sekunde die Liste der zu speichernden Daten um ‚Passwörter‘ (mots de passe) ergänzt worden. (…) Der ~~europäische~~ Chefdatenschützer von Google, Peter Fleischer (…) bringt die Konsequenzen gut auf den Punkt: Damit ist der Einstieg gemacht in die Vorratsdatenspeicherung von Inhalten, während es bisher ja ’nur‘ um Verbindungsdaten ging.“

Vorratsdatenspeicherung dient der Telefonseelsorge

Der neue Bundesinnenminister ist super.

Deutschlandfunk heute mittag (ab etwa 3:40):
„Es dürfte sie nicht überraschen, dass ich, was die Notwendigkeit der Vorratsdatenspeicherung betrifft, der gleichen Auffassung bin wie mein Vorgänger, dass wir effizient auch das Instrumentarium nutzen, was möglich ist, um Terrorismusverbrechen zu bekämpfen und deswegen denke ich wird es wichtig sein, dass wir möglichst schnell auch beim Thema VDS zu einem Ergebnis kommen."

Focus Offline:
„Die Freiheit der Bürger sei heute aber nicht mehr bedroht durch einen Obrigkeitsstaat. Heute komme es darauf an, dass Kriminelle und Verbrecher nicht ‚die Oberhand gewinnen' und dass Deutschland nicht zum Rückzugsort für Terroristen werde. Ermittler müssten auch die Möglichkeit haben herauszufinden, was für Kontakte ein Verdächtiger in den letzten Monaten gehabt habe. (…) Auch könne Menschen in seelischen Notlagen, beispielsweise bei einer Selbstmordankündigung übers Telefon, ‚durch einen schnellen Zugriff auf Verkehrsdaten geholfen werden', sagte Friedrich weiter.

Man muss also ohne Anlass die Kommunikationsdaten aller Bürger für sechs Monate speichern, weil es der Telefonseelsorge dient.

Boykottiert de-mail!

Der Bundestag, hat wie zu erwarten war, das De-Mail-Gesetz verabschiedet.

Auf datenspeicherung.de kann man detailliert nachlesen, warum man diesen Unfug auf jeden Fall boykottieren sollte – hier nur wenige Zitate:

„Aufgrund der Architektur von De-Mail fließen alle Daten und Kontakte auf die Person rückführbar an einer zentralen Stelle zusammen;.. (…) Die hinterlegten persönlichen Daten des Nutzers sind für eine Vielzahl von Sicherheitsbehörden und Geheimdiensten ohne richterliche Anordnung anforderbar (§ 113 TKG), die Identität hinter einer De-Mail-Adresse ist für über 1.000 Behörden in einem Onlineverfahren abrufbar (§ 112 TKG (…) Eine Vorratsspeicherung der Verbindungsdaten jeder De-Mail (vgl. § 100 TKG) schließt der Gesetzentwurf nicht aus. Kennung und Passwort zu einem De-Mail-Postfach sind auf Anforderung einer Strafverfolgungsbehörde, einer Polizeibehörde, des Bundesamts für Verfassungsschutz, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes ohne richterliche Anordnung herauszugeben (§ 113 TKG). (…)“

Was Vorratsdaten über uns verraten

Zeit.de: „Interpol und Deutsche Bank, FBI und Scotland Yard, Flensburg und das BKA, haben unsere Daten da“, sangen Kraftwerk 1981 in Computerwelt. Es klang damals unglaublich, später bedrohlich, und heute klingt es lächerlich. (…)

Der Grünenpolitiker Malte Spitz hat sich daher entschlossen, seine Vorratsdaten aus dem Zeitraum August 2009 bis Februar 2010 zu veröffentlichen. Um sie zu überhaupt bekommen, musste er gegen die Telekom klagen. Die Daten, die *Zeit Online* hier zum Download zur Verfügung stellt und die Basis der hier gezeigten interaktiven Karte sind, entstammen einem Exceldokument mit 35.831 Zeilen. Mehr als 35.000 Mal also hat sein Mobiltelefon in diesem halben Jahr Informationen Preis gegeben… (…)

Vorratsdaten zeigen, wer Freund ist und wer Familie, sie bringen geheime Liebschaften ebenso ans Licht wie verborgene Netzwerke."

(Vorsicht! Um die interaktive Karte ansehen zu können, muss man Javascript erlauben: Man muss sich von googleapis.com, von gstatic.com und google.com ausspionieren lassen. Das verrät uns *Zeit online* aber nicht, es wird als selbstverständlich vorausgesetzt.)

Indect – der Wiedergänger der negativ-dekadenten Persönlichkeit

Das „abnormale Verhalten", nach dem INDECT sucht, hieß in der DDR „negativ-dekadente Persönlichkeit". „Internet child pornography, promotion of totalitarian symbols, trafficking in human organs, spread of botnets, viruses, malware. Alle bekannten Sprechblasen vorhanden. Quod erat demonstrandum.

Vorratsdatenspeicherung light plus [Update]

Kurt Biedenkopf, Ex-Generalsekretär der CDU, soll 1973 gesagt haben: „Was sich heute in unserem Land vollzieht, ist eine Revolution neuer Art. […] Revolutionen finden heute auf andere Weise statt. Statt der Gebäude der Regierungen werden die Begriffe besetzt, mit denen sie regiert."

Richtig: Wenn man dem politiischen Gegner die eigenen Begriffe und Definitionen aufzwingt, dann infiltriert man ihn auch mit den eigenen Ideen. Bundesjustizministerin Sabine Leutheusser-Schnarrenberger versucht es gerade wieder, einerseits, um der Überwachungs- und Zensurmafia die halbherzige FDP-Position schmackhaft zu machen, andererseits um die Gegner der Vorratsdatenspeicherung ins Leere laufen zu lassen.

Vorratsdatenspeicherung heisst jetzt *Quick Freeze Plus*. Jawoll. Folter heisst jetzt „rubuste Wahrheitssuche", das Atommüllager nennen wir jetzt „Entsorgungspark", und den Krieg kennen wir ohnehin schon als „Friedenserzwingung".

Noch mal zum Mitschreiben: „Vorratsdatenspeicherung bezeichnet die Verpflichtung der Anbieter von Telekommunikationsdiensten zur Registrierung von elektronischen Kommunikationsvorgängen, ohne dass ein Anfangsverdacht oder eine konkrete Gefahr besteht (Speicherung bestimmter Daten auf Vorrat)."

Die Regierung will alle Verkehrs- und Kommunikationsdaten aller Bürger auf Vorrat sammeln – ohne konkreten Anlass. Im Prinzip ist die Richtlinie 2006/24/EG der Europäischen über die Vorratsspeicherung von Daten schuld; wie diese Vorgabe juristisch umgesetzt wird, bleibt den Mitgliedsstaaten überlassen. Das deutsche Bundesverfassungsgericht erklärte die

deutschen Vorschriften – also den ersten Versuch zur Vorratsdatenspeicherung – mit seinem Urteil vom 2. März 2010 für verfassungswidrig und nichtig.

Das interessiert die Zensur- und Überwachungsmafia und deren politischen Lautsprecher natürlich nicht. Und Leutheusser-Schnarrenberger ist nur so eine Art feministische Theologin: Sie versucht, das Falsche, Lächerliche, Böse noch irgendwie angenehm zu kostümieren und uns schmackhaft zu machen. Mit der Vorratsdatenspeicherung ist es aber wie mit der Schwangerschaft – ein bisschen geht nicht.

Wie absurd die Diskussion mittlerweile ist, zeigt das Beispiel: Welche Reaktion würde jemand ernten, der forderte, alle Jogger und sonstigen Fußgänger würden ab sofort generall überwacht und ihre Wegstrecken protokolliert werden, weil man auf diese Weise auch zu Fuß flüchtende Bankräuber erwischen würde? Genau so argumentieren die Befürworter der Vorratsdatenspeicherung. Was offline gilt, muss auch online gelten: Anonymität im Internet ist ein Bürgerrecht!

Die German Privacy Foundation hat das so formuliert: „Die zunehmende Überwachung der Kommunikation erfordert das Recht auf und den Schutz der Privatsphäre. Die Freiheit in der digitalen Welt muss verteidigt werden. Das Recht auf ungehinderte Kommunikation ist ein Menschenrecht, das Recht auf informationelle Selbstbestimmung, also auch auf Anonymität, ein unverzichtbares Bürgerrecht und eine Grundfeste des Datenschutzes. Jeder hat das Recht, selbst zu entscheiden, welche Informationen er oder sie über sich selbst preisgibt. Solange nicht ein staatliches Gesetz oder die Rechte anderer entgegenstehen, kann jeder Mensch sein Recht auf informationelle Selbstbestimmung in der Form ausüben, dass er anonym auftritt und sich insbesondere im Internet anonym bewegt.“

Update: Vgl. Thomas Stadler: „Die Vorratsdatenspeicherung ist aus grundsätzlichen rechtsstaatlichen Erwägungen heraus

abzulehnen und es hat dabei zu bleiben, dass deutschen Ermittlungsbehörden nicht dieselben Imstrumente an die Hand gegeben werden dürfen, wie den Behörden totalitärer Staaten. Zudem wäre wünschenswert, dass die Diskussion um die Vorratsdatenspeicherung stärker in den Kontext des Datenschutzes gestellt wird. Denn die Politik kann nicht einerseits ein hohes Datenschutzniveau, das nur durch die gesetzlich normierten Ziel der Datenvermeidung und Datensparsamkeit erreichbar ist, propagieren und andererseits eine Vorratsdatenspeicherung fordern.“

Datenspionage ist obligatorisch [2. Update]

Golem.de berichtet: „Hamburgs Datenschutzbeauftragter, Johannes Caspar, hat seinen Internetauftritt abschalten lassen, da auf der Seite ‚unzulässige Trackingsoftware‘ zum Einsatz kam.“

Echten Datenschutz gibt es offenbar nur, wenn man gar nicht mehr kommuniziert. Har har. Rechtsanwalt Thomas Stadler hatten dem Datenschutzbeauftragten die Leviten gelesen: Unter

datenschutz-hamburg.de werde „Tracking-Technologie eingesetzt“ und „kräftig getrackt“.

„Stadler spielte auf das in den Seiten integrierte IVW-Pixel an, mit dem die Informationsgemeinschaft zur Feststellung der Verbreitung von Werbeträgern die Reichweiten vieler deutscher Websites misst, auch die von Golem.de. Die Teilnahme am Messverfahren der IVW ist für größere Websites, die sich über Werbevermarktung finanzieren, auf dem deutschen Markt praktisch obligatorisch.“

Aha. Gut zu wissen. Die Formulierung ist verräterisch: „praktisch obligatorisch“? Das heisst: Alle tun es, aber keiner möchte darüber reden? Dazu passt ja die heuchlerische Titelgeschichte im aktuellen Print-Spiegel – mit „Datenkraken“ sind immer nur die anderen gemeint.

Abhilfe gegen Tracking schafft das Firefox-Add-on ghostery. Ihr werdet euch wundern, wie viele Websites plötzlich nicht mehr „korrekt“ angezeigt werden bzw. meckern, dass ihr angeblich „veraltete“ oder „falsche“ Browser benutzt. Derartige Add-ons sind ein Sargnagel für das Internet-Geschäftmodell auch deutscher Medien. Deswegen empfiehlt die niemand.

[*Update*] Besonders dreist ist die taz: „Auch taz.de hat den Zählpixel von INFOnline für IVW auf seiner Website integriert. **Was genau sie dabei erheben, inwieweit sie anonymisieren, das steht außerhalb der direkten Kontrolle von taz.de** und allen anderen Kunden-Websites.“ Dann ist ja alles gut.

[*2. Update*] Die Süddeutsche verschweigt in einem linkfreien Artikel sogar, dass sie selbst diese Tracker nutzt (vgl. den Quelltext von sueddeutsche.de).

Piratenpartei Hessen spendet TOR-Server an die GPF

Bad Vilbel online – Rhein Main News: „Seit Ende letzten Jahres läuft ein von der Piratenpartei Hessen gesponsorter Anonymisierungsserver bei der German Privacy Foundation. Die Adminstration des neuen TOR-Exit-Nodes „gpfTOR4“ erfolgt in Zusammenarbeit durch die Piratenpartei Hessen (1. Admin) und die GPF (2. Admin). (…) ‚Durch einen weiteren Server leisten wir einen Beitrag für sichere und vertrauenswürdige TOR-Exit-Nodes. Wir möchten an dieser Steller der renommierten German Privacy Foundation dafür danken, dass sie als Betreiber und Berater zur Verfügung stehen“ erklärte Ralf Praschak, Stellvertretender Vorsitzender der Piratenpartei Hessen. „Gerade in Zeiten, in denen über die Wiedereinführung der Vorratsdatenspeicherung diskutiert wird und Ungarn eine Zensur innerhalb der EU beschlossen und umgesetzt hat, ist dies nötiger denn je.'“

Erschütternden Inkompetenz

Ich wollte eigentlich zu dem Thema, dass Twitter aufgefordert wurde, Nutzerdaten von Wikileaks-Sympathisanten herauszurücken, etwas bloggen. Aber Feynsinn hat alles Nötige dazu schon gesagt, auch zu den Journalisten-DAUs, die beim Freitag hanebüchenen Unfug verbreiten. Mich erschüttert die Inkompetenz jedoch eher nicht, ich erwarte es geradezu – deutsche Journaille eben.

„Mir ist völlig klar, dass ich mich mit meinen andauernden Rufen nicht beliebt mache und muss sogar davon ausgehen, dass

die Mehrheit meiner Leser einen Facebook-Account hat," schreibt Feynsinn. Bei mir macht er sich beliebt, und ich habe auch keinen Facebook-Accout mehr.

Torservers.net: Warum es so wichtig ist

Interessanter Artikel über Tor:

„Tor ist eben kein einfaches Anonymisierungsprojekt nur für ‚uns'. Mit staatlicher Förderung und vor allem viel persönlichem Engagement wird und wurde an Universitäten (und außerhalb) weltweit daran gearbeitet, allen Menschen einen zensurfreien, verschlüsselten Netzzugang zu ermöglichen. Und das in seiner vollen Konsequenz: Nicht nur lesend, sondern auch um aktiv teilzunehmen, ohne Repressalien fürchten zu müssen. Auf der Startseite von Torservers.net zitiere ich eine Studie des ‚Commitee to Protect Journalists', nach der im letzten Jahr 136 Journalisten weltweit im Gefängnis sitzen. Und das sind nur die bekannteren Fälle.

Und, wird Tor genutzt? Und von wem? Die Metriken des Torprojekts zeigen das sehr eindrucksvoll. Wenn man sich nämlich dort anschaut, wie viele Menschen den umständlichen Weg nutzen, sich Tor per Email zu besorgen – vermutlich weil die Seite des Projekts geblockt wird und somit der normale Downloadweg nicht möglich ist – so sind das knapp 100 täglich".

Lesebefehl!

Verschlüsselung Ihrer E-Mail gefährdet unser Mitlesen

Ich bin sprachlos. Troll, troller, am Trollsten. Das hier ist die offizielle Position der Bundesregierung:

„‚Die Nachrichten werden zur Überprüfung von Viren und zur Prüfung, ob es sich um eine Spam-Mail handelt, kurzfristig entschlüsselt', heißt es in der Stellungnahme. Während dieses Vorgangs seien die Nachrichten einem ‚erhöhten Risiko des Angriffes durch unbefugte Dritte ausgesetzt'. Die Bundesregierung stimmt diesem Bundesrats-Vorschlag in ihrer mit der Unterrichtung ebenfalls vorgelegten Gegenäußerung nicht zu. ‚Eine Ende-zu-Ende-Verschlüsselung gefährdet das gesamte Ziel von De-Mail, die einfache – und ohne spezielle Softwareinstallation mögliche – Nutzbarkeit durch die Bürgerinnen und Bürger', argumentiert sie in der Vorlage."

Das ist nicht nur grober Unfug, sondern schlicht Volksverdummung. Guckst du auch hier: „Für die Verschlüsselung von E-Mails muss der jeweilige Absender den öffentlichen Schlüssel des Empfängers in seinen E-Mail-Client einbinden. Der öffentliche Schlüssel für die jeweilige E-Mail-Adresse der Abgeordneten und Verwaltungsmitarbeiter ist automatisch in jeder signierten E-Mail des Abgeordneten oder Mitarbeiters enthalten. Gegebenenfalls bitten Sie Ihren Kommunikationspartner im Deutschen Bundestag Ihnen eine signierte E-Mail zu senden, um ihm verschlüsselt antworten zu können." (Die Realität sieht natürlich anders aus)

Das erinnert mich an Google Mail: „Unser System, wie z. B. unsere Spamfilter, durchsucht den Inhalt Ihrer Nachrichten automatisch nach Keywords, damit wir Ihnen nur relevante

Informationen liefern“.

Das sollte die Bundesregierung doch gleich sagen: „Unser System De-Mail entschlüsselt ihre E-Mails kurz und durchsucht den Inhalt Ihrer Nachrichten automatisch nach verdächtigen Keywords wie „Bombenbauanleitung“ oder „Kinderpornografie“. E-Mails dieser Art werden automatisch gelöscht, damit wir Ihnen nur relevante Informationen liefern.“

Sogar bei golem.org schreiben sie Quatsch zum Thema: „Wenn der Anwender eine De-Mail an einen anderen De-Mail-Teilnehmer verschickt, wird diese kurzzeitig auf den De-Mail-Servern entschlüsselt und wieder verschlüsselt. Dabei wird die Verbindung zum Nutzer per SSL verschlüsselt, diese Verschlüsselung aber auf Serverseite terminiert. Geschäftskunden, die über ein Gateway an De-Mail angeschlossen sind, können die Ende-zu-Ende-Verschlüsselung über bestehende Systeme wie S/MIME oder PGP durchführen. Für Privatkunden ist aktuell nur die Möglichkeit gegeben, auf Fileebene verschlüsselte Daten an eine De-Mail als Attachment anzuhängen, etwa mit Truecrypt verschlüsselte Dokumente.“

Mannomann. Was für Trantüten. E-Mail-Attachments mit Truecrypt verschlüsseln? „Free open-source disk encryption software for Windows 7/Vista/XP, Mac OS X, and Linux.“ Disk encryption – *nicht* E-Mails oder Files verschlüsseln. Wer Lesen kann, ist klar im Vorteil.

(Via netzpolitik.org u.a.)

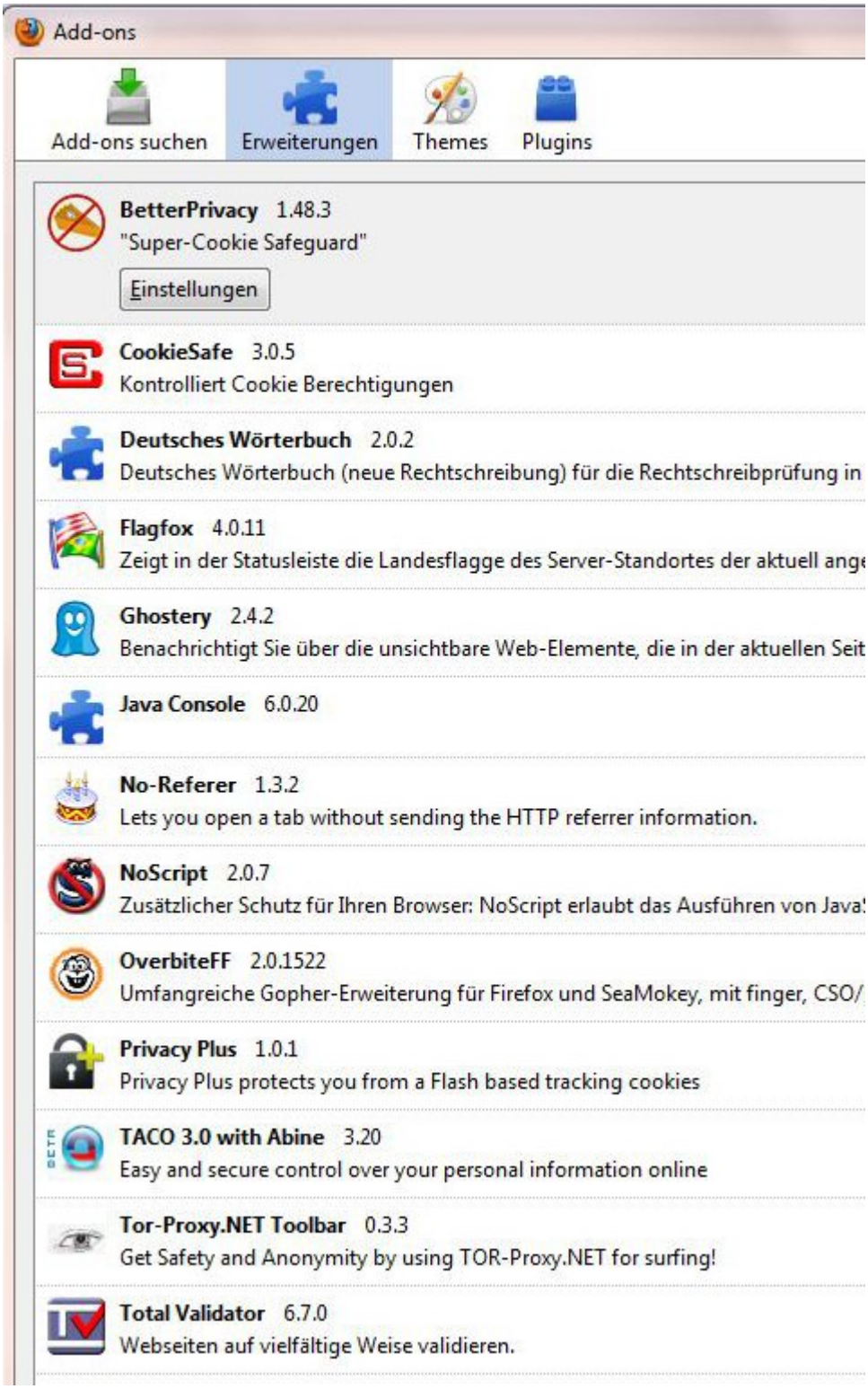
PrivacyBox, revisited

Heise über Whistleblower-Plattformen und die Privacybox der German Privacy Foundation, „das älteste System dieser Art“:

„‚Die ursprüngliche Intention, dass (Online-)Journalisten ihre Privacybox-Kontaktseite als Kontaktmöglichkeit für Whistleblower anbieten, scheint sich nicht erfüllt zu haben. Zumindest sind uns keine Postfächer bekannt, die von Medien wie heise online genutzt werden,‘ erklärte Neß.“

Das hätte mal jemand den Leyendecker fragen sollen, obb er weiß, was die PrivacyBox ist oder wie man wikileak anonym Unterlagen zu schicken könnte. Es gibt schon einige wenige Kollegen, die das System nutzen. Aber der Rest lebt wie gewohnt hinter dem Mond, vom Verschlüsseln der E-Mails ganz zu schweigen. Deutscher Journalismus eben.

Browser-„Lücken“ – Experte ist nicht alarmiert



Ich musste bei der Lektüre des Spiegel „Online“-Artikels heftig schmunzeln (Immerhin ein externer Link, o Wunder – aber es ist auch bald Weihnachten). Ich bin ja „Experte“, bin aber im Gegensatz zur These des Spiegel-Autors *nicht* „alarmiert“ über die pöhsen Kriminellen, die uns ausspionieren.

Es gibt nur *ein* Computerproblem – das hat zwei Ohren und sitzt

vor dem Monitor. Des Extremistenforum burks.de rät: Installieren Sie diese Add-ons! Machen Sie nicht? Quod erat demonstrandum.

Eine rote Linie, die jeder beachten muss

Tagesschau.de: „Das Internet wird in Birma, China, Iran, Nordkorea, Turkmenistan und Vietnam weltweit am schärfsten zensiert. Zu diesem Ergebnis kommt eine Studie der US-Universität Kansas, aus der die Fachzeitschrift „GeoJournal“ zitiert.“

Natürlich ist tagesschau.de zu blöd oder zu faul oder zu feige („öffentlich-rechtliche *Anstalt*„) , irgendwelche Links zu setzen, etwa zu dem zitierten Professor Barney Warf. Witzig ist hingegen die Kreiszeitung – Böblinger Bote (whois): „Der Download des Warf-Artikels ‚Geographies of global Internet censorship‘ (Geografien der globalen Internet-Zensur) in ‚GeoJournal‘ ist nur für Abonnenten oder per Einmalzahlung einer Gebühr möglich“ mit dem Hinweis: „Download des Artikels, PDF, 1 MB, 34 Euro“. Vierunddreissig Euro. Das ist doch mal ein Geschäftmodell einer deutschen Zeitung! Es bezieht sich aber auf springer.com, wo das pdf eben so viel kostet – immerhin kein Surplusprofit…

Das *abstract* bei springer.com lautet: „More than one-quarter of the planet’s population uses the Internet today, although access to it is highly uneven throughout the world. While it is widely celebrated for its emancipatory potential, many governments view the Internet with alarm and have attempted to limit access or to control its contents. This project seeks to

provide a comprehensive, theoretically informed analysis of the geographies of Internet censorship. It begins by clarifying the reasons, types, extent of, and opposition to, government limitations of Internet access and contents. Invoking an index of censorship by Reporters Without Borders, it maps the severity of censorship worldwide and assesses the numbers of people affected, and using the Freedom House index, it correlates political liberty with penetration rates. Second, it explores Internet censorship at several levels of severity to explicate the multiple means through which censorship is implemented and resisted. The third part offers a moral critique of Internet censorship via a Habermasian interpretation of cyberspace as the closest real-world approximation of an ideal speech situation. The summary notes the paradox of growing e-government and continued fears of an expanded domain of public discourse."

Das bringt es sehr schön auf den Punkt. Es ist ein Paradoxon, dass Regierungen von „E-government" reden und gleichzeitig das Internet zensieren und den Diskurs der Bürger dort fürchten.

Deutschland und seine *German Intenet Angst*™ sind das beste Beispiel. Die

„Das Linux-Magazin berichtet in seiner Ausgabe 12/2010 über den CryptoStick: „Open-Source-Hardware ist keine Spielerei, das zeigt ein USB-Stick der German Privacy Foundation." Neben einer kurzen Erläuterung der im Stick verbauten Technik beschreibt der Artikel, wie man den Stick unter Linux in Betrieb nimmt und mit dem GNU Privacy Guard einsetzt." (GPF)