Totalüberwachungs-Lobbyist Uhl ist merkbefreit

Laut FAZ belegen die Vorfälle in Toulouse den „Bedarf an Vorratsdaten“.

Uhl, der das behauptet hat, lügt und dummschwätzt. Aber das ist man von einem Lobbyisten der Wollt-Ihr-die-totale-Überwachung ja gewohnt.

Patrick Breyer schreibt: „Entgegen anders lautender Falschmeldungen haben die französischen Ermittler den Serienmörder von Toulouse ohne Vorratsdatenspeicherung identifiziert.“

Das Max-Planck-Institut stellte bereits vor Monaten fest: „Die Entwicklung von Aufklärungsraten und Fällen bei Morddelikten zeigt eine beständige Abnahme der Fallzahlen ab Anfang der 1990er Jahre und eine entsprechende Zunahme der Aufklärungsquote. Auch hier ergibt sich kein Hinweis darauf, dass sich die Vorratsdatenspeicherungin sichtbarer Weise ausgewirkt haben könnte.“

Sicherheit im Internet

Vortrag und Workshop „Sicherheit im Internet“: pdf zum Download

---

Cryptoportal

„Das Cryptoportal bietet Lehrern eine Plattform, auf der sie Unterrichtsmaterialien zum Thema Informationssicherheit und Kryptologie veröffentlichen und darüber diskutieren können. Dadurch sollen gegenseitige Anregungen und Hilfen sowohl für Lehrer als auch für Lernende entstehen.“

Unter Fernwartern

Zwei hübsche Meldungen bei Heise, die irgendwie zusammenpassen:
„Sämtliche Windows-Versionen via Remote Desktop angreifbar“ – das ist natürlich eine irreführende Schlagzeile, aber das hier erklärt alles:

Zwar ist der Remote-Desktop-Server (alias Remotedesktopverbindung) standardmäßig nicht aktiv, die praktische Fernwartungsfunktion erfreut sich jedoch großer Beliebtheit und ist in vielen Fällen auch über das Internet erreichbar.

LMAO.

Zwar ist die unverschlossene Haustür standardmäßig nicht aktiv, die praktische Funktion erfreut sich jedoch großer Beliebtheit und ist in vielen Fällen auch über öffentliche Straßen erreichbar.

Und hier: Studie: Mangelnde IT-Kenntnisse hemmen Unternehmenserfolg.

Nicht nur den Unternehmenserfolg, aucn die Berichterstattung der Medien über alles, was mit dem pöhsen Internet

zusammenhängt.

Digitales Aikido: Wie schütze ich meine Daten im Internet?

Der DJV Berlin richtet in Kooperation mit der German Privacy Foundation am Mittwoch, 21. März 2012 um 19 Uhr in der Geschäftsstelle des DJV Berlin (Taubenstr. 20, Berlin-Mitte), ein Seminar aus zum Thema:

Sicheres Surfen – Verschlüsselte E-Mail: Wie schütze ich meine Daten im Internet? – Vortrag und Workshop mit Burkhard Schröder

Was ist zu beachten, um Daten auf einem Computer zu schützen? Wie kann man E-Mails verschlüsseln und wann ist es nötig? Wie kann man sicher surfen?

Angesprochen sind vor allem Kolleginnen und Kollegen, die sich bisher nicht für das Thema Sicherheit interessiert haben. Vorkenntnisse sind nicht erforderlich. Laptops können mitgebracht werden.

Zur Person: Burkhard Schröder ist stellvertretender Vorsitzender des Fachausschusses Online beim DJV Berlin und Mitbegründer der German Privacy Foundation.

Die Teilnahme ist kostenlos, die Teilnehmerzahl ist begrenzt. Bitte melden Sie sich an: info@djv-berlin.de, Sie erhalten eine Bestätigung.

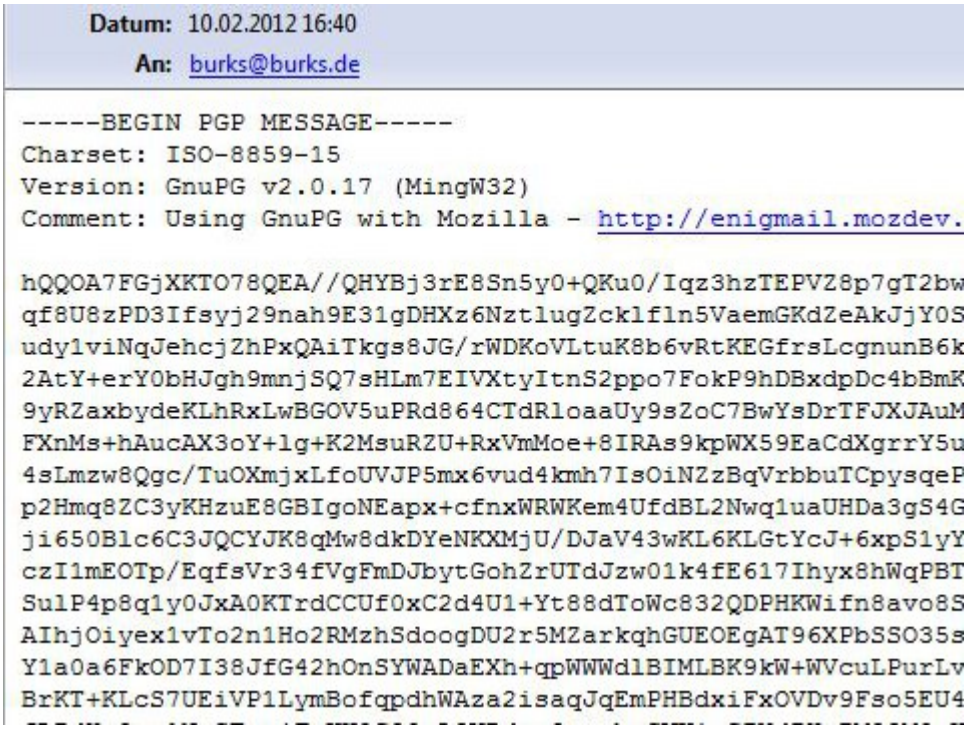
Obzora! Nenore! Oybjwbof! Gnyvona! Nany!

vpu jüeqr zrvar Znvyf zvg ubputenqvtre, süe qvr Fpuynccuügr tnenagvreg hayrfonere Uvtugrpu-Fgnaqneg-(ahe rpug zvg qrz g!)-Irefpuyüffryhat orunaqrya. Fbyyra fvr qbpu xbzzra! XnybevraOBZOR! FrkOBZOR!

Evpugvt! EBG13 zvg Ibyyovg-Irefpuyüffryhat. Qnaa xöaafr haf nyyr zny!

Nhf qrz Urvfr-Sbehz uggc://jjj.urvfr.qr/arjfgvpxre/sbera/F-Er-Also-wnrre-ich-Bombenbauer/sbehz-222870/zft-21491367/ernq/

Hilfe! Die Geheimdienste lesen meine E-Mails!



Datum: 10.02.2012 16:40
An: burks@burks.de

```
-----BEGIN PGP MESSAGE-----
Charset: ISO-8859-15
Version: GnuPG v2.0.17 (MingW32)
Comment: Using GnuPG with Mozilla - http://enigmail.mozdev.

hQQOA7FGjXKTO78QEA//QHYBj3rE8Sn5y0+QKu0/Iqz3hzTEPVZ8p7gT2bw
qf8U8zPD3Ifsyj29nah9E31gDHXz6NztlugZcklfln5VaemGKdZeAkJjY0S
udy1viNqJehcjZhPxQAiTkgs8JG/rWDKoVLtuK8b6vRtKEGfrsLcgnunB6k
2AtY+erY0bHJgh9mnjSQ7sHLm7EIVXtyItnS2ppo7FokP9hDBxdpDc4bBmK
9yRZaxbydeKLhRxLwBGOV5uPRd864CTdRloaaUy9sZoC7BwYsDrTFJXJAuM
FXnMs+hAucAX3oY+lg+K2MsuRZU+RxVmMoe+8IRAs9kpWX59EaCdXgrrY5u
4sLmzw8Qgc/TuOXmjxLfoUVJP5mx6vud4kmh7IsOiNZzBqVrbbuTCpysqeP
p2Hmq8ZC3yKHzuE8GBIgoNEapx+cfnxWRWKem4UfdBL2Nwq1uaUHDa3gS4G
ji650Blc6C3JQCYJK8qMw8dkDYeNKXMjU/DJaV43wKL6KLGtYcJ+6xpS1yY
czI1mEOTp/EqfsVr34fVgFmDJbytGohZrUTdJzw01k4fE617Ihyx8hWqPBT
SulP4p8q1y0JxA0KTrdCCUf0xC2d4U1+Yt88dToWc832QDPHKWifn8avo8S
AIhjOiyex1vTo2n1Ho2RMzhSdoogDU2r5MZarkqhGUEOEgAT96XPbSSO35s
Y1a0a6FkOD7I38JfG42hOnSYWADaEXh+qpWWWdlBIMLBK9kW+WVcuLPurLv
BrKT+KLcS7UEiVP1LymBofqpdhWAza2isaqJqEmPHBdxiFxOVDv9Fso5EU4
```

SpOn: „Bei der Fahndung nach Terroristen, Waffenschiebern oder Schleuserbanden hat der deutsche Geheimdienst im Jahr 2010 einem Bericht zufolge insgesamt 37.292.862 E-Mails und Datenverbindungen überprüft. (…) Trotz der massenweisen Überwachung habe es nur in 213 Fällen tatsächlich verwertbare Hinweise für die Geheimdienste gegeben.“

Ach?

BVerfG: Telekommunikationsgesetz teilweise verfassungswidrig [Update]

Pressemitteilung des Bundesverfasungsgerichts über eine aktuelle Entscheidung (Az.: 1 BvR 1299/05) – Tenor:

„Regelungen des Telekommunikationsgesetzes zur Speicherung und Verwendung von Telekommunikationsdaten teilweise verfassungswidrig“.

1. In der Zuordnung von Telekommunikationsnummern zu ihren Anschlussinhabern liegt ein Eingriff in das Recht auf informationelle Selbstbestimmung. Demgegenüber liegt in der Zuordnung von dynamischen IP-Adressen ein Eingriff in Art. 10 Abs. 1 GG.

2. Der Gesetzgeber muss bei der Einrichtung eines Auskunftsverfahrens sowohl Rechtsgrundlagen für die Übermittlung, als auch für den Abruf von Daten schaffen.

3. Das automatisierte Auskunftsverfahren der §§ 112, 111 TKG ist mit der Verfassung vereinbar. § 112 TKG setzt dabei für den Abruf eigene Ermächtigungsgrundlagen voraus.

4. Das manuelle Auskunftsverfahren der §§ 113 Abs. 1 Satz 1, 111, 95 Abs. 1 TKG ist in verfassungskonformer Auslegung mit dem Grundgesetz vereinbar. Zum einen bedarf es für den Abruf der Daten qualifizierter Rechtsgrundlagen, die selbst eine Auskunftspflicht der Telekommunikationsunternehmen normenklar begründen. Zum anderen darf die Vorschrift nicht zur Zuordnung dynamischer IP-Adressen angewendet werden.

5. Die Sicherheitsbehörden dürfen Auskünfte über Zugangssicherungscodes (§ 113 Abs. 1 Satz 2 TKG) nur dann verlangen, wenn die gesetzlichen Voraussetzungen für ihre Nutzung gegeben sind.

Schon wieder eine Klatsche für die Überwachungslobby. Ganz entzückend. Bundesverfassungsgericht, you made my day and my weekend.

[Update] Eine Analyse zum Urteil im *law blog*.

Das Ministerium für Google-Wahrheiten informiert:

Datenspionage heisst jetzt „den vollen Funktionsumfang haben“.

Das Wall Street Journal, von dem deutsche Medien alles abgeschrieben haben: „Google Inc. and other advertising companies have been bypassing the privacy settings of millions of people using Apple Inc.’s Web browser on their iPhones and computers – tracking the Web-browsing habits of people who intended for that kind of monitoring to be blocked.“

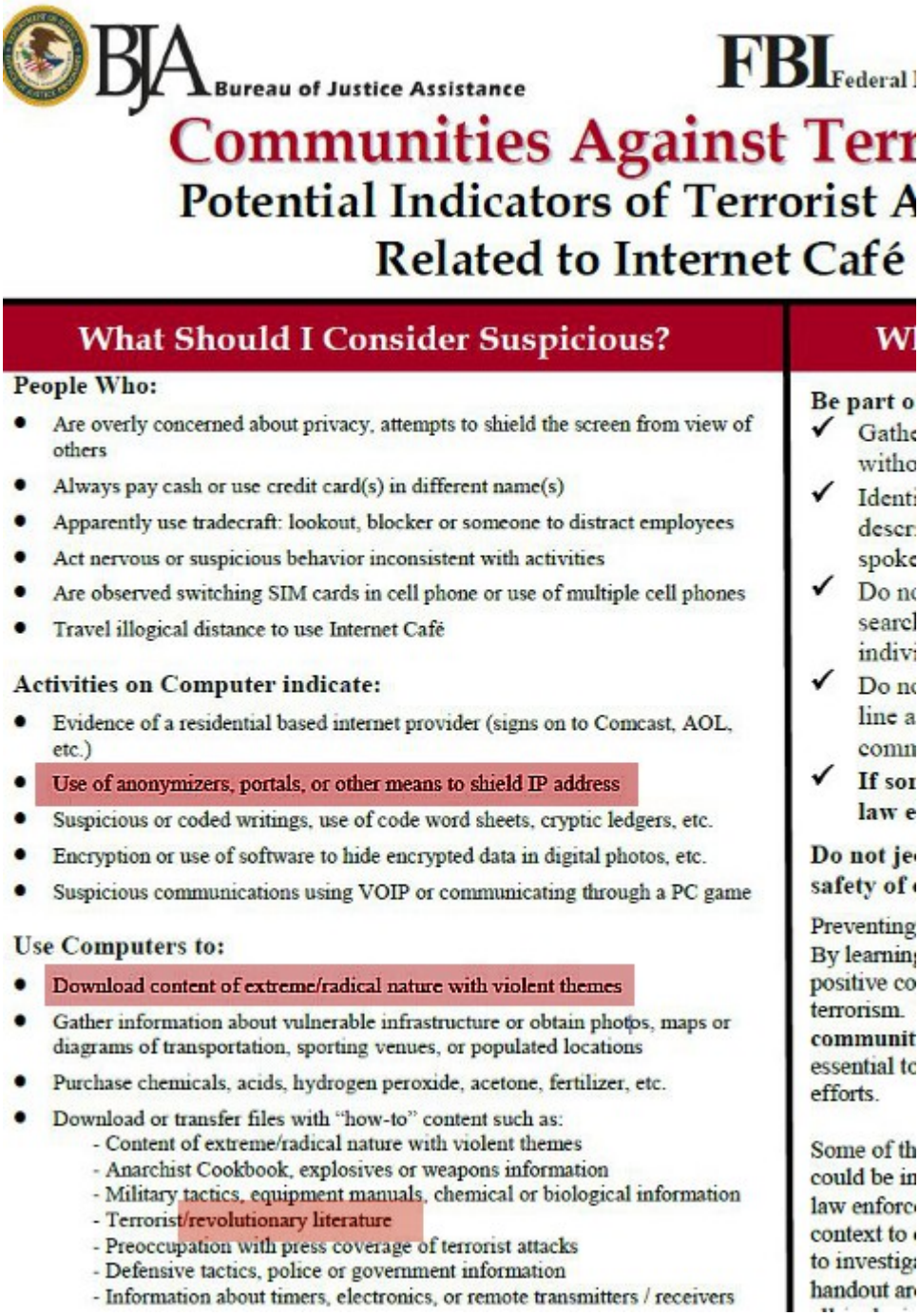
Das Ministerium für Googles Wahrheit informiert: Datenspionage heisst jetzt Datenschutz

Datenschutzerklärung von Google – das muss man nicht weiter kommentieren. Wer sich das gefallen lässt, ist eine Pappnase.
u.a.:
Gerätebezogene Informationen
Wir erfassen möglicherweise gerätespezifische Informationen (beispielsweise das von Ihnen verwendete Hardware-Modell, die Version des Betriebssystems, eindeutige Gerätekennungen und Informationen über mobile Netzwerke, einschließlich Ihrer Telefonnummer). Google verknüpft Ihre Gerätekennungen oder

Telefonnummer gegebenenfalls mit Ihrem Google-Konto. (…)
Einzelheiten zu der Art und Weise, wie Sie unsere Dienste genutzt haben, beispielsweise Ihre Suchanfragen.
Telefonieprotokollinformationen wie Ihre Telefonnummer, Anrufernummer, Weiterleitungsnummern, Datum und Uhrzeit von Anrufen, Dauer von Anrufen, SMS-Routing-Informationen und Art der Anrufe.
IP-Adresse.
Daten zu Geräteereignissen wie Abstürze, Systemaktivität, Hardware-Einstellungen, Browser-Typ, Browser-Sprache, Datum und Uhrzeit Ihrer Anfrage und Referral-URL.
Cookies, über die Ihr Browser oder Ihr Google-Konto eindeutig identifiziert werden können. (…)
Gegebenenfalls erheben und speichern wir Informationen (einschließlich personenbezogene Daten) lokal auf Ihrem Gerät, indem wir Mechanismen wie beispielsweise den Webspeicher Ihres Browsers (einschließlich HTML 5) und Applikationsdaten-Caches nutzen.

Guckst du auch hier, wie das u.a. zu umgehen sei. (Das reicht aber noch nicht.)

Do You Like Online Privacy? You May Be a Terrorist



BJA Bureau of Justice Assistance

FBI Federal

Communities Against Terr

Potential Indicators of Terrorist A

Related to Internet Café

What Should I Consider Suspicious?

People Who:

- Are overly concerned about privacy, attempts to shield the screen from view of others
- Always pay cash or use credit card(s) in different name(s)
- Apparently use tradecraft: lookout, blocker or someone to distract employees
- Act nervous or suspicious behavior inconsistent with activities
- Are observed switching SIM cards in cell phone or use of multiple cell phones
- Travel illogical distance to use Internet Café

Activities on Computer indicate:

- Evidence of a residential based internet provider (signs on to Comcast, AOL, etc.)
- Use of anonymizers, portals, or other means to shield IP address
- Suspicious or coded writings, use of code word sheets, cryptic ledgers, etc.
- Encryption or use of software to hide encrypted data in digital photos, etc.
- Suspicious communications using VOIP or communicating through a PC game

Use Computers to:

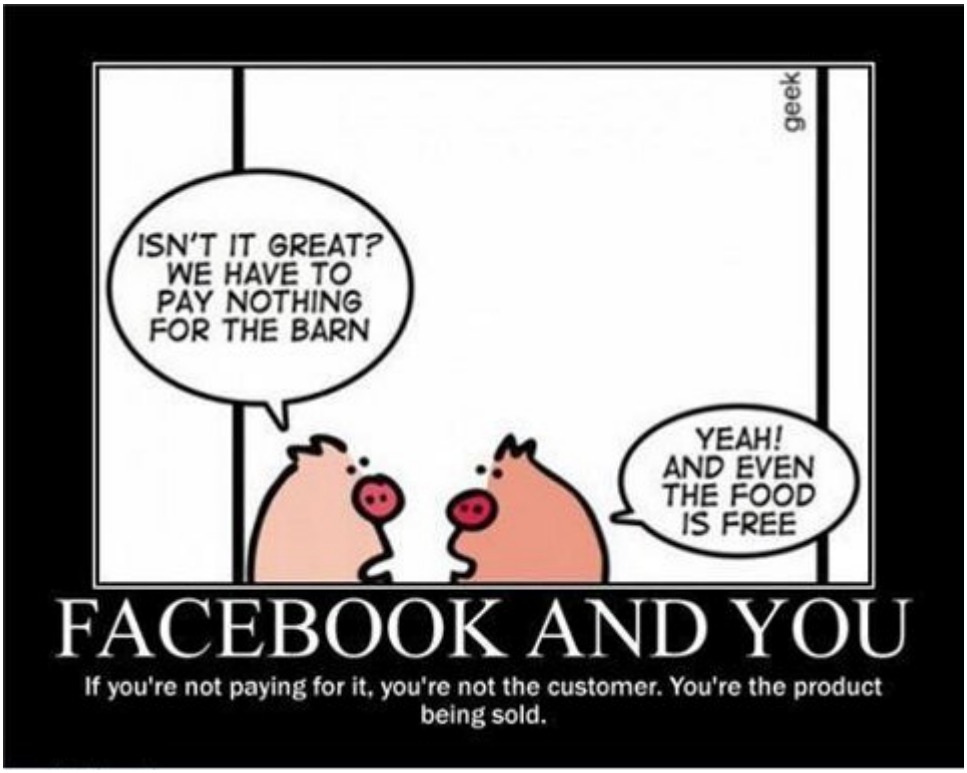
- Download content of extreme/radical nature with violent themes
- Gather information about vulnerable infrastructure or obtain photos, maps or diagrams of transportation, sporting venues, or populated locations
- Purchase chemicals, acids, hydrogen peroxide, acetone, fertilizer, etc.
- Download or transfer files with "how-to" content such as:
  - Content of extreme/radical nature with violent themes
  - Anarchist Cookbook, explosives or weapons information
  - Military tactics, equipment manuals, chemical or biological information
  - Terrorist/revolutionary literature
  - Preoccupation with press coverage of terrorist attacks
  - Defensive tactics, police or government information
  - Information about timers, electronics, or remote transmitters / receivers

Warum beschweren die sich über die Internet-Zensur in China? In den USA sind sie ja genau so paranoid. Wenn ich dort Karl Marx in einem Internet-Cafe läse oder Tor benutzte, würde ich vermutlich verhaftet. (Via public intelligence)

Viva Comandante Camila Vallejos!

Die linke chilenische Studentenführerin Camila Vallejos kritisiert die Telefonüberwachung und die Zensur der Presse. Viva Chile! (By the way: Die Linke hatte immer die schönsten und intelligentesten Frauen!)

Fratzenbuch



(Danke, Ruben!)

Nicht wirklich Neues von der Überwachungs-Lobby

Mitteldeutsche Zeitung: „Das Bundeskriminalamt (BKA) kann wegen des Verzichts auf die Vorratsdatenspeicherung in Deutschland nicht so effektiv gegen die rechtsterroristische Zelle „Nationalsozialistischer Untergrund“ ermitteln, wie es das gerne tun würde.“

Liebe Mitteldeutsche Zeitung, wenn du die Agitprop der Überwachungs-Lobby schon eins zu eins und ohne ein kritisches Wort dazu abdruckst, dann wähle doch bitte die korrekte grammatikalische Form „könne“. Die behaupten das nur, es stimmt gar nicht. Also muss hier die indirekte Rede stehen: Die sagen, es sei so. Es ist aber nicht so und wir glauben es überhaupt nicht. Begründung:

Die [[x] irgendeine Überwachungs-Behörde, bitte selbst ausfüllen] kann wegen des Verzichts auf die Vorratsdatenspeicherung folgendes nicht tun: [[x] bitte selbst ausfüllen]: Das Böse aus der Welt vertreiben, Hütchenspieler verhaften, Drogenschmuggel unterbinden, Nazis bekämpfen, die Parteiführung der Linken beobachten, gestohlene Autos wiederfinden, Wirtschaftskriminelle auf die Seite der Guten herüberziehen, Kinderpornografie aus der Welt schaffen, das Internet totalüberwachen, Heuschrecken und das Finanzkapital in die Schranken weisen, Handtaschenräüber dingfest machen, Omas über die Straße helfen, bei Facebook nach Verbrechern fahnden u.v.a.m..

Big Brother (NOC) is watching you

Via Fefe, Yahoo und TV-Novosti (RTД):
Under the National Operations Center (NOC)'s Media Monitoring Initiative that emerged from the Department of Homeland Security in November, Washington has written permission to collect and retain personal information from journalists, news anchors, reporters or anyone who uses "traditional and/or social media in real time to keep their audience situationally aware and informed. (…)

Specifically, the DHS announced the NCO and its Office of Operations Coordination and Planning (OPS) can collect personal information from news anchors, journalists, reporters or anyone who may use "traditional and/or social media in real time to keep their audience situationally aware and informed. (…)

According to RT, the website "Fast Company" reports that the NOC Monitoring Initiative has been in play since at least early-2010 and **that the data is being shared with both private sector businesses and international third parties**.

Massenhafte Funkzellenabfrage jetzt auch in Berlin

Netzpolitik.org: „Dass die Dresdner Aktion nur die Spitze des Eisbergs ist, verdeutlicht ein neuer Fall aus Berlin. Wir haben Akten (PDF) erhalten, die eine weitere massenhafte Abfrage von Mobilfunk-Daten belegen. Ende 2009 haben Polizei

und Staatsanwaltschaft die “Erfassung und Übermittlung sämtlicher Verkehrsdaten und Verbindungsdaten” eines Stadtgebiets angefordert und bekommen.“ (mehr…)

Anhand der persönlichen Surf-History

Heise: „Googles Suchmaschine durchsucht künftig auch die Inhalte des eigenen Google-Plus-Profils und bezieht verstärkt Inhalte aus dem Sozialen Netzwerk in die Ergebnisliste mit ein (…) Mit einer neuen Schaltfläche – dem Weltkugel-Button oben rechts – lassen sich diese neuen Features auch wieder abschalten. Das betrifft auch die „Web History“, mit der Google anhand der persönlichen Surf-History versucht, die Treffergenauigkeit zu verbessern, *selbst wenn der betreffende Nutzer nicht eingeloggt ist*.“

Kann mir mal jemand *eine* Person nennen, die dem Datenkranken Google freiwillig erzählt, wo man was und wann angesurft hat? Wer das tut, leidet doch an geistiger Umnachtung oder ist nur einfach unsäglich dämlich. Aber davon gibt es ja genug.

Das Ministerium für Wahrheit informiert: Ausspionieren heisst jetzt „die Treffergenauigkeit verbessern“.

DJV Berlin: Diskussion über

Datenkraken

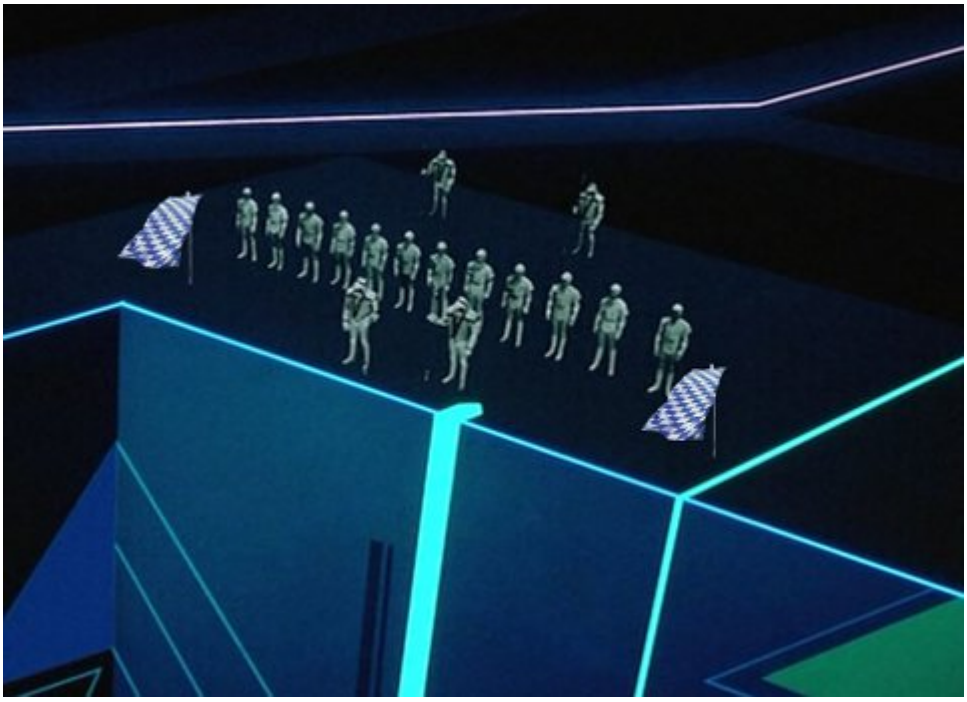
Der Fachausschuss Online des DJV Berlin lädt zu einem Diskussionsabend mit dem Berliner Datenschutzbeauftragten Dr. Alexander Dix in die Geschäftsstelle des DJV Berlin (Taubenstr. 20, 10117 Berlin) ein.

Am 24. Januar 2012 um 19.00 Uhr spricht Herr Dr. Dix zum Thema „Sicherheit für Journalisten im Internet“. Dabei stellt er die Kernfrage: „Werden wir von den Datenkraken übertölpelt? Gefahren und Risiken von Facebook & Co. Wie vorsichtig muss man als Journalist sein?“.

Im Anschluss beantwortet Dr. Dix Fragen und steht für eine Diskussionsrunde zur Verfügung. Der Abend wird moderiert von Burkhard Schröder.

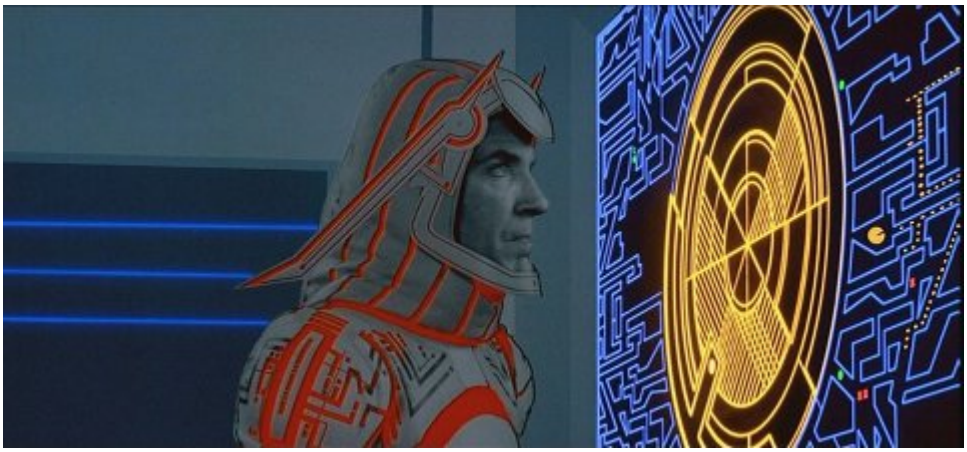
Über eine kurze Teilnahmebestätigung an info@djv-berlin.de würden wir uns freuen.

Bayerische Cyberpolizei



Heise meldet: „Bayern will mit speziell ausgebildeten „Internetpolizisten“ gegen die [*angeblich, B.S.*] zunehmende Kriminalität im Netz vorgehen. (…) Herrmann mahnte deshalb, wenn man Spuren von Tätern im Internet sichern wolle, müsse man auf die Verbindungsdaten zurückgreifen können. Man müsse beispielsweise identifizieren können, wer hinter einer IP-Adresse stecke.“

Exklusiv auf burks.de hier erste Fotos der bayerischen Cyberpolizei. Oben: Morgenandacht der Beamten. Unten: Ein bayerischer Cyberpolizist untersucht eine festgenommene IP-Adresse.



BKA imitiert China

Heise: „Das Bundeskriminalamt (BKA) hat eine Zugriffsblockade auf seine Webseite für Nutzer von Virtual Private Networks wieder aufgehoben, nachdem sich der Bundesdatenschutzbeauftragte eingeschaltet hat. (…) Laut Telemediengesetz (TMG) sind Diensteanbieter verpflichtet, die Nutzung von Online-Medien ‚anonym oder unter Pseudonym zu ermöglichen'."

So fühlt man Absicht und man ist verstimmt. Was in den Gesetzen steht, interessiert das BKA einfach nicht. Zu dumm, um in dieselben zu schauen, sind sie ja nicht. Die würden bei einem rechten Putsch in Deutschland widerspruchslos weitermachen. Pack.