

Dienstag, 30. September 2008

Baden-Württembergischer Datenschutzbeauftragter kritisiert Videoüberwachung an Mannheimer Schulen

Der baden-württembergische Landesdatenschutzbeauftragte Peter Zimmermann hat die Videoüberwachung an Mannheimer Schulen (siehe diesen Blogeintrag) in einer Stellungnahme scharf kritisiert.

Laut Peter Zimmermann fehlt für die Videoüberwachung die nach dem Urteil des Bundesverfassungsgerichts im Jahr 2007 notwendige gesetzliche Grundlage für eine Videoüberwachung mit Speicherung der Aufzeichnungen. Auch wenn das Urteil zu einem Sachverhalt in Bayern ergangen sei, sei es grundsätzlich auch in Baden-Württemberg anwendbar. Für Altanlagen, die vor dem Urteil errichtet worden waren, sei eine Übergangsfrist denkbar, deren Ende er aber spätestens Ende 2008 sieht. Wenn die Videoüberwachung fortgeführt werden solle, müsste der Landtag erst eine gesetzliche Grundlage schaffen.

Die Stadt Mannheim will nun laut dem SWR vorerst nur die 4 Neuanlagen abschalten, an den 13 Altanlagen läuft die Videoüberwachung vorerst weiter. Hier hätte die Stadt Mannheim einen klaren Schnitt ziehen können - schließlich kommen zahlreiche andere Städte im "Ländle" ohne Videoüberwachung aus. Mannheim will laut stimme.de wird die "Einzelfälle prüfen" - Rückzugsgefecht anstatt klarem Schnitt.

Geschrieben von Stefan in Datenschutz um 21:05

Und täglich grüßt das Murmeltier: Datenpanne in Großbritannien

In unserer Reihe Datenpannen in Großbritannien präsentieren wir heute: die Geheimdienstkamera bei ebay.

Ein 28jähriger hat auf ebay eine Digitalkamera ersteigert, teuer war sie auch nicht, umgerechnet 21 Euro. Er freut sich und nimmt die Kamera mit in den Urlaub. Wieder zu Hause lut er die Bilder auf den PC und entdeckte zwischen den Urlaubsfotos unter anderem Bilder von Raketenabschussrampen, Al-Quaida-Verdächtigen (inkl. Namen und Fingerabdrücken) - vermutlich Bilder des britischen Auslandsgeheimdienstes MI6. Er wurde stutzig und ging zur Polizei. Ein paar Tage später statteten ihm dann Geheimdienstbeamte einen Besuch ab und beschlagnahmten die Kamera.

Merke: wer an geheime Daten will, muss einfach nur nach Großbritannien gehen...

Via Spiegel
Online und heise.de

Geschrieben von Stefan in Datenschutz um 20:29

Montag, 29. September 2008

Kontroverse Meinungen zum Vorgehen der Telekom bei Verbindungsdatenweitergabe

Am Freitag fand sich im Blog von Patrick Breyer der Eintrag, die Telekom würde gegen einen von ihm gestellten Antrag vorgehen, den Verwaltungsakt der Bundesnetzagentur öffentlich zu machen, mit dem die Telekom die Herausgabe von Verbindungsdaten ohne richterliche Anordnung begründet (siehe den entsprechenden Eintrag vom Samstag).

Die taz stellt den Vorgang nun ganz anders dar: Laut der taz geht die Telekom nicht gegen die Veröffentlichung, sondern gegen den Verwaltungsakt selbst vor, der sie zu der illegalen Herausgabe der Verbindungsdaten zwingt.

Ein Telekom-Sprecher wird wie folgt zitiert:

Damit müssen wir quasi gegen das Fernmeldegeheimnis verstoßen

Deswegen haben wir beim Verwaltungsgericht Köln einen Eilantrag auf Aussetzung dieser Regelung gestellt.

Die Bundesnetzagentur verteidigt den Verwaltungsakt als notwendig, um die Nutzer zu identifizieren. Der Verwaltungsakt

regelt auch nur die sofortige Auswertung und längere interne Speicherung der Daten bei der Telekom und nicht die Herausgabe und sei daher vom Telekommunikationsgesetz abgedeckt.

Was nun richtig ist, muss wohl die Zeit zeigen. Aber selbst wenn sich die Sichtweise der taz bestätigt, bleibt der Vorwurf bestehen, dass die Telekom (mindestens einmal) Verbindungsdaten ohne richterliche Genehmigung an die Staatsanwaltschaft weitergegeben hat.

Hier die Einträge in der taz und dem CTRL-Blog, sowie der ursprüngliche Blogeintrag von Patrick Breyer.

Geschrieben von Stefan in Datenschutz um 08:50

Samstag, 27. September 2008

Überwachte die Telekom auch Emails?

Heise.de und futureZone melden mit Berufung auf den Spiegel, dass die Telekom neben den Festnetz- und Mobilfunkverbindungen von Journalisten und gewerkschaftlichen Aufsichtsratsmitgliedern auch Emails überwacht hat. Dafür lägen konkrete Hinweise vor, die sich aus Dokumenten ergeben, die die Bonner Staatsanwaltschaft vorliegen hat. Laut dem Spiegel soll die Konzernsicherheit der Telekom auch Zugriff auf den gesamten Emailverkehr des Konzerns gehabt haben. Der damalige Telekom-Chef Kai-Uwe Ricke soll angeblich in einem Gespräch mit Gewerkschaftern Zugriff auf Unterlagen gehabt haben, die vorher vertraulich per Mail versandt worden waren. Mehr auf heise.de und futureZone.

Geschrieben von Stefan in Datenschutz um 12:33

Welch Überraschung: Mal wieder Festplatten mit Daten in Großbritannien abhanden gekommen (Update 29.9.)

Wie futureZone meldet, hat das britische Verteidigungsministerium bekannt gegeben, dass auf dem Luftwaffenstützpunkt Innsworth drei Festplatten mit den persönlichen Daten von mehreren tausend Militärangehörigen gestohlen wurden. Die Festplatten wurden im Hochsicherheitsbereich des Stützpunktes aufbewahrt - sehr viel Sicherheit scheint nicht vorhanden zu sein. Wieviele Daten genau verschwunden sind, ist noch gar nicht klar, auf dem Stützpunkt werden die Daten von 900.000 Militärangehörigen verwaltet.

Der Vorfall reiht sich ein in eine ganze Reihe von Fällen in Großbritannien in den letzten Monaten. Erst gestern war bekannt geworden, dass eine CD mit 11.000 Daten von britischen Lehrern verschwunden ist.

Update: Spiegel Online und heise.de melden, dass USB-Sticks gestohlen wurden, keine Festplatten.

Geschrieben von Stefan in Datenschutz um 11:01

Telekom stemmt sich gegen Klarheit bei Verbindungsdaten (Update 29.9.)

Der Telekom wurde Anfang des Monats von Patrick Breyer in seinem Blog vorgeworfen, dass sie illegal und ungefragt Verbindungsdaten herausgibt, noch dazu unzulänglich verschlüsselt (siehe den Eintrag hierzu).

Die Geschichte scheint sich nun "interessant" zu entwickeln. Patrick Breyer fragte beim Bundesdatenschutzbeauftragten nach und eine Mitarbeiterin bestätigte, dass diese Praxis illegal sei und dass die Telekom zugesagt habe, das Verfahren zu ändern. Nachdem die Meldung auch auf heise.de zu lesen war, haben einige Leser Strafanzeige gegen die Telekom wegen

Verstoßes gegen das Fernmeldegeheimnis erstattet. Die Telekom beruft sich nun auf einen Verwaltungsakt der Bundesnetzagentur - als ob ein Verwaltungsakt der Netzagentur die Gesetzeslage ändern könnte. Patrick Breyer versucht

nun, diesen Verwaltungsakt nach dem Informationsfreiheitsgesetz einzusehen.

Pikanterweise geht die Telekom nun gerichtlich gegen die Herausgabe vor. Offensichtlich scheint man bei der Telekom selbst nicht davon überzeugt zu sein, dass dieser Verwaltungsakt das Verhalten der Telekom rechtfertigt, andernfalls würde dieses Gerichtsverfahren ja kontraproduktiv sein.

Patrick Breyer vermutet, dass die Telekom einen zweiten Datenschutzskandal und weitere Strafverfahren verhindern will

-
was anhand der vorliegenden Informationen sehr plausibel scheint.

Genauer Infos im Blog von Patrick Breyer.

Update: Die taz schreibt nun in einem Artikel, gerichtlich gegen den Verwaltungsakt selbst vorgeht und sich als Opfer sieht. Mehr dazu hier.

Geschrieben von Stefan in Datenschutz um 10:38

Freitag, 26. September 2008

Erneuter Datenverlust in Großbritannien (Update)

Laut futureZone ist eine CD mit tausenden Datensätzen in Großbritannien verloren gegangen. Eine britische Lehrerorganisation meldete den Verlust einer CD mit 11.000 Datensätzen. Laut der Organisation seien aber keine finanziellen Daten enthalten und die CD sei verschlüsselt.

Den Lehrern bleibt nur zu wünschen, dass sie gut verschlüsselt wurde...

Update: heise.de meldet noch ein paar Details zu dem Verlust. So wurde die CD mit Daten wohl per Kurier versandt, kam aber nie am Bestimmungsort an. Bei einer Durchsuchung des Fahrzeugs war sie auch nicht mehr aufzufinden.

Geschrieben von Stefan in Datenschutz um 09:50

Donnerstag, 25. September 2008

Unzulässige Videoüberwachung an Mannheimer Schulen

Die Stuttgarter Zeitung meldet, dass an Mannheimer Schulen seit Jahren ohne Gesetzesgrundlage Eingänge, Pausenhöfe und Flure überwacht werden.

Die ersten Videokameras seien 1995 installiert worden, mittlerweile würde an 17 von 95 öffentlichen Mannheimer Schulen überwacht. Teilweise würden die Aufnahmen bis zu 2 Wochen aufbewahrt. Herausgekommen ist dies durch eine Anfrage der Grünen im Mannheimer Gemeinderat. Der baden-württembergische Datenschutzbeauftragte bereitet zur Zeit eine Stellungnahme vor. Er beurteilt die Maßnahme aber als "nicht unkritisch", da das Bundesverfassungsgericht im Februar 2007 entschieden hatte, dass eine Überwachung öffentlicher Plätze nur mit gesetzlicher Grundlage erlaubt ist, die auch nach der Schwere des Grundrechtseingriffs angemessen ist. In Baden-Württemberg gibt es allerdings keine rechtliche Grundlage für Videoüberwachung an Schulen.

Weder Innen- noch Kultusministerium in Baden-Württemberg haben auf eine Anfrage der Zeitung geantwortet, an wievielen

Schulen denn eine Videoüberwachung installiert sei. Anfragen in einigen Städten ergab allerdings, dass sich diese Städte aufgrund der Rechtslage gegen die Überwachung entschieden hatten.

Geschrieben von Stefan in Datenschutz um 17:59

AK Vorratsdatenspeicherung veröffentlicht Datenaustauschabkommen mit den USA

Der AK Vorratsdatenspeicherung hat das bisher geheim gehaltene Abkommen zum Datenaustausch mit den USA veröffentlicht.

Der AK verbindet die Veröffentlichung mit einem Aufruf an die Bundestagsabgeordneten, dem Abkommen nicht zuzustimmen.

Es sei europaweit einzigartig und der Datenschutz in keinsten Weise gesichert.

Die ganzen Kritikpunkte liest man am Besten in der Erklärung des AK Vorratsdatenspeicherung nach.

Zusätzlich noch 2 Dinge, die mir (als Nicht-Jurist) beim Durchlesen des Abkommens auffielen:

Im Artikel 10 "Übermittlung personenbezogener und anderer Daten zur Verhinderung terroristischer Straftaten" (3) Mit der Notifikation nach Artikel 24 Satz 1 können die Vertragsparteien einander in einer gesonderten Erklärung die Straftaten notifizieren, die nach ihrem innerstaatlichen Recht als Straftaten im Sinne des Absatzes 1 gelten. Die Erklärung nach Satz 1 kann jederzeit durch eine Notifikation gegenüber der anderen Vertragspartei geändert werden.

Das heißt: die Straftaten, die eine Datenabfrage zur Terrorabwehr zulassen, können jederzeit einseitig geändert/ausgeweitet werden. Pikanterweise könnte die deutsche Seite die Abfrage noch nicht einmal sofort unterbinden, sollten die USA die "terroristisch relevanten" Straftaten deutlich ausweiten. Im Abkommen ist eine Kündigungsfrist von 3 Monaten vorgesehen.

Im Artikel 15: "Dokumentation"

(3) Die Protokolldaten sind durch geeignete Vorkehrungen gegen zweckfremde Verwendung und sonstigen Missbrauch zu schützen und zwei Jahre aufzubewahren. Nach Ablauf der Aufbewahrungsfrist sind die Protokolldaten unverzüglich zu löschen, soweit innerstaatliches Recht einschließlich anwendbarer Datenschutz- und Datenaufbewahrungsvorschriften nicht entgegensteht.

Das heißt, wenn keine anderen Vorschriften dem entgegen stehen, werden die Protokolle über die Zugriffe nach 2 Jahren gelöscht. Die übertragenen Vergleichsdaten müssen zwar unmittelbar nach dem Vergleich gelöscht werden - es sei denn, sie sind zur Abwendung einer ernsthaften Bedrohung für die innere Sicherheit erforderlich. Die übertragenen personenbezogenen Daten dürfen aber solange aufbewahrt werden wie nötig. Da in den Protokollen aber z.B. auch steht,

an welche Stellen die Daten weitergegeben wurden, ist nach 2 Jahren überhaupt nicht mehr nachzuweisen, welchen Weg die Daten genommen haben. Auf der anderen Seite ist dies vermutlich sowieso nicht mehr von großem Belang, sobald sich die Daten in den USA befinden.

Geschrieben von Stefan in Datenschutz um 12:11

Mittwoch, 24. September 2008

Telekompaket passiert Europaparlament mit Einschränkungen

Laut futureZone hat das Telekom-Paket das Europaparlament passiert, allerdings mit einer wichtigen Einschränkung: die Regelung "Three Strikes and you're out", die Provider dazu verpflichten sollte, bei der dritten Urheberrechtsverletzung ihrer Kunden den Anschluss zu sperren, wurde abgelehnt. Diese vor allem von französischer Seite

forcierte Regelung war im Vorfeld heftig kritisiert worden, da sie eine umfassende Überwachung der User durch die Provider erfordert.

Allerdings heißt das nicht, dass die Regelung nun europaweit vom Tisch ist. Vielmehr bleibt es den einzelnen Mitgliedsstaaten überlassen, ob sie eine solche Regelung einführen. Die Provider sollen aber zur Zusammenarbeit mit den Rechteinhabern verpflichtet werden. Allerdings wurde auch ein kurzfristig eingebrachter Änderungsantrag angenommen, dass Rechte und Freiheiten der Internetnutzer nur mit Zustimmung eines Richters beschnitten werden dürfen, schreibt heise.de.

Laut heise.de wird es nun vermutlich nach einer Stellungnahme der französischen EU-Ratspräsidentschaft von einer zweiten Lesung des Telekom-Pakets abhängen, was tatsächlich in der EU Realität werden wird.

Update: Mittlerweile gibt es auch eine erste Einschätzung von netzpolitik.org.

Geschrieben von Stefan in Datenschutz um 15:07

Europaparlament stimmt für mehr Datenschutz

Das Europaparlament hat gestern für mehr Datenschutz gestimmt und die Vereinbarung des EU-Ministerrates kritisiert. Die

Angleichung von Justizbestimmungen in den Ländern der EU dürfe nicht zu Lasten des Datenschutzes gehen. Mit großer

Mehrheit wurde der Bericht von Martine Roure gebilligt, der den Vorschlag der Innenminister in vielen vor allem datenschutz-relevanten Punkten verschärft.

Mehr Infos finden sich auf futurezone, golem.de, heise.de und Telepolis.

Bleibt nur zu hoffen, dass der Datenschutz auch bei der heutigen Abstimmung zum Telekom-Paket eine Rolle spielen wird.

Mehr zum Hintergrund auf netzpolitik.org, auch ein Artikel auf Spiegel Online widmet sich der heutigen Abstimmung.

Geschrieben von Stefan in Datenschutz um 14:20

Blick ins Ausland: Terrorabwehr gegen Kleinstdelikte und Datenbanken für alles

"Eine ewige Erfahrung lehrt, dass jeder Mensch, der Macht hat, dazu getrieben wird, sie zu missbrauchen. Er geht immer weiter, bis er an Grenzen stößt."

(Charles de Montesquieu, Vom Geist der Gesetze)

Vor ein paar Tagen haben sowohl Spiegel Online als auch Zeit Online den Missbrauch der Anti-Terror-Gesetze in Großbritannien berichtet.

Der Regulation of Investigatory Powers Act (RIPA) gab den Behörden das Recht Emails mitzulesen, Telefon- und Internetverbindungen zu überwachen, Kontoauszüge einzusehen, Videoüberwachung durchzuführen oder die Herausgabe von

Passwörtern zu verlangen. Im Jahr 2003 wurden der Kreis der berechtigten Behörden drastisch ausgeweitet. Seitdem können auch Gemeinden, Schulbehörden oder Arbeitsämter Überwachungen durchführen und Informationen einsehen, nur

die Telefonüberwachung bleibt den Sicherheitsbehörden vorbehalten. Ein belegter Verdacht muss nicht vorliegen, es reicht ein (anonymer) Hinweis.

Dieses Recht wird offensichtlich auch ausgiebig genutzt, zu jedem denkbaren nichtigen Anlass. Der Daily Telegraph meldete im April, dass jeden Monat 1000 neue

Ausspionierungsaktionen durch die Gemeinden gestartet werden. Was alles dafür Anlass bietet, ist mehr als bizarr. So

wurde eine komplette Familie in Poole mit allen Mitteln der Technik überwacht, nur weil der Verdacht besteht, sie hätten ihr Kind im falschen Schulbezirk angemeldet. Später stellte sich heraus, dass sie aus dem Schulbezirk verzogen waren und ihre Kinder mit Billigung des Direktors in der Schule belassen hatte. Allein dieses Beispiel zeigt, wie sorglos mit den Möglichkeiten der Überwachung in Großbritannien umgegangen wird, durch eine kurze Nachfrage hätte der Sachverhalt aus der Welt geschafft werden können. Leider handelt es sich hier aber um keinen Einzelfall, in Derby wurden Videokameras aufgestellt, nachdem sich Anwohner über spielende Kinder beschwert hatten.

Noch ein paar Beispiele aus dem Artikel von Spiegel Online:

- In Easington begann die Stadt, den Garten eines Anwohners zu überwachen, weil sich seine Nachbarn über Lärm beschwert hatten.

- In Newcastle überwachte die Stadtverwaltung die Praxis eines Tierarztes, weil Nachbarn über bellende Hunde klagten.

- In Durham holte die Stadt die Genehmigung ein, Privatpersonen zu überwachen, die Dinge auf dem Flohmarkt verkauften, um Warenfälschern auf die Spur zu kommen.

- Die Stadtverwaltung von Westminster (London) überwachte einen Schlosser, weil er des Betrugs bezichtigt worden war.

- Der Torbay City Council las die E-Mails eines Angestellten mit, weil er beschuldigt wurde, "verdächtiges Material" verschickt zu haben. Einem zweiten Angestellten wurde hinterherspioniert, weil er angeblich einen Wagen der Stadtverwaltung für Privatzwecke genutzt hatte.

- In Canterbury wurde ein Ermittler auf Privatpersonen angesetzt, die im Verdacht standen, illegal mit Pizza zu handeln.

Selbst der Polizei wird die Überwachung mittlerweile zuviel. Die ständige Überwachung würde die eigenen Ermittlungen gefährden, die Regierung solle die Befugnisse doch wieder einschränken, kommen Stimmen aus der Polizei.

Bürgerrechtsgruppen in Großbritannien vergleichen die Verhältnisse mittlerweile mit China oder der deutschen Stasi.

Während es der Überwachung in den USA auch genug gibt, hat ein weiterer Spiegel Online-Artikel sich den allumfassenden Datenbanken in den Vereinigten Staaten gewidmet.

In den Public Record Databases finden sich z.B. Vorstafen, Verkehrsvergehen oder einfach Daten, die normalerweise geschützt sind wie z.B. Wohnorte von Prominenten. Entweder ganz kostenlos oder gegen eine geringe Gebühr lässt sich

alles herausfinden. Verwechslungen wegen Namensgleichheit sind natürlich immer möglich. Dagegen wirkt rottenneighbor.com fast harmlos - trotzdem kein Grund die Seite gut zu finden...

Geschrieben von Stefan in Datenschutz um 12:54

Freitag, 19. September 2008

Interview mit Sven Gábor Jánszky in der taz

Über den Eintrag im CTRL-Blog hatte ich ja schon etwas geschrieben. Nun findet sich in der taz ein kurzes Interview mit Sven Gábor Jánszky.

Gegenüber dem Blog-Eintrag allerdings nicht viel Neues, er wiederholt nur seine Thesen, dass die Menschen den Datenschutz für die Vorteile (wie z.B. Rabatte) selbst aufgeben werden und der Datenschutz nur noch gegen kriminelle Aktivitäten wirken wird.

Das Interview findet ihr auf den Seiten der taz.

Geschrieben von Stefan in Datenschutz um 13:06

Nachwehen des Datenschutzgipfels

Der Datenschutzgipfel Anfang September wirkt immer noch nach. Die Oppositionsparteien werfen der Regierung vor, es nicht ernst zu meinen und auf halbem Wege halt zu machen. Außerdem werfen sie Bundesinnenminister Schäuble vor, dass sich die angebliche Stärkung des Datenschutzes nicht auf den Haushalt auswirkt: dem Bundesdatenschutzbeauftragten würde außer einer tariflichen Gehaltsanpassung keine weiteren Haushaltsgelder bewilligt - obwohl der Etat des Innenministeriums um 10% steigt. Sie versuchen durch Anträge die Bundesregierung in Zugzwang zu bringen.

Die Datenschützer des Bundes und der Länder haben die Bundesregierung aufgefordert, die beschlossenen Maßnahmen zügig umzusetzen - wohl auch, um die öffentliche Aufmerksamkeit und den dadurch bestehenden Druck auszunutzen und zu verhindern, dass die Beschlüsse "verwässert" werden. Auch müssten die Datenschutzbeauftragten finanziell und personell besser ausgestattet werden.

Geschrieben von Stefan in Datenschutz um 12:33

Stiftung Warentest-Buch zum Datenschutz im Alltag

Die Stiftung Warentest hat ein Buch herausgegeben, dass sich mit dem Datenschutz im Alltag beschäftigt.

Für 12,90 € lässt sich das Buch "Meine Daten schützen" im Buchhandel bestellen, das sich unter anderem mit dem Internet oder dem Einkaufen.

Mehr Infos gibt es auf den Seiten der Stiftung Warentest.

Geschrieben von Stefan in Datenschutz um 10:07

Donnerstag, 11. September 2008

c't-Hintergrund zu Statewatch-Report

Während der deutschen EU-Ratspräsidentschaft wurde von Bundesinnenminister Schäuble eine Arbeitsgruppe eingesetzt, die Pläne für eine künftige EU-Innenpolitik entwickeln sollen. Statewatch hat die Pläne analysiert und warnt vor einem Big-Brother-Szenario mit völligem Wegfall der Privatsphäre. Ein c't-Hintergrund geht auf den Hintergrund und den Statewatch-Report ein.

Unter anderem heißt es dort:

Dass heutzutage der Standort jedes aktiven Mobiltelefons überwacht werden kann, ist demnach "erst der Anfang" der neuen Datensammelmöglichkeiten. In den kommenden Jahren würden Milliarden Geräte aus der physischen Welt miteinander über RFID, WLAN, Wimax, Bluetooth oder ZigBee verknüpft werden. Dies gestatte es, immer mehr Objekte in

Echtzeit zu verfolgen. In naher Zukunft würden die meisten Gegenstände digitale Datenströme über ihren Ort und ihre Nutzung generieren und somit letztlich Verhaltensmuster ihrer Anwender offenbaren. Diese könnten von Sicherheitsexperten für die Verhinderung oder Untersuchung von Vorfällen verwendet werden.

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.

Den ganzen Artikel findet ihr hier.

Geschrieben von Stefan in Datenschutz um 13:32

Bußgeldbescheide in Höhe von 1,42 Millionen für Lidl verschickt

Wie bereits angekündigt haben die Datenschutzbeauftragten der Länder die Bußgeldbescheide für Lidl wegen der Bespitzelungsaffäre verschickt.

Aus der Pressemitteilung des Unabhängigen Datenschutzbüros:

Die für die 35 Lidl-Vertriebsgesellschaften in Deutschland zuständigen zwölf Datenschutzaufsichtsbehörden haben bei der Überprüfung dieser Gesellschaften schwerwiegende Datenschutzverstöße

festgestellt und Bußgelder in einer Gesamthöhe von 1,462 Mio. Euro festgesetzt. Nachdem im März 2008 über Medien bekannt wurde, dass Lidl-Mitarbeiterinnen und -Mitarbeiter systematisch durch Sicherheitsunternehmen überwacht worden

waren, wurden in den Datenschutzbehörden Ermittlungen eingeleitet, die nunmehr mit Bußgeldbescheiden abgeschlossen werden.

Der Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) sieht in den Bescheiden eine Stärkung des Datenschutzes. Auch sei durch den Skandal die Aufmerksamkeit der Öffentlichkeit für den Datenschutz gewachsen.

Die koordinierenden Datenschützer aus Baden-Württemberg haben auch eine Pressemitteilung herausgegeben, die auf den Seiten des Unabhängigen Datenschutzbüros abrufbar ist (.pdf).

Ob allerdings wirklich ein langfristiges Umdenken der Verbraucher einsetzt, darf meiner Meinung im Moment noch bezweifelt werden...

Blog Export: Überwachungsorgan, <http://www.pfadefinden.org/blog/>

Geschrieben von Stefan in Datenschutz um 13:15

Mittwoch, 10. September 2008

Zukunftsvision: Bequemlichkeit führt zu Ende des Datenschutzes?

Im CTRL-Blog findet

sich ein Brief von Sven Gábor Jány, Leiter des Think-Tanks "forward2business". Er stellt ohne auf mögliche Risiken oder Missbrauch einzugehen die vernetzte Zukunft im Jahr 2020 dar.

Besonders nett die Antwort auf die Frage, warum wir uns auf diese Vernetzung einlassen werden:

Weil wir wissen, dass der Nutzen überwiegt. Wir erhalten Rabatte oder Anerkennung und haben kaum etwas zu befürchten außer ein paar Werbebriefen und Werbemails, die ungelesen in den Müll wandern.

Ich schlieÙe nicht aus, dass viele die von ihm dargestellte Vernetzung wirklich nutzen - man sieht ja, wie viele Menschen ihre Daten über Payback und weitere "Kundenkarten" für Rabatte zwischen 0,3 und 4% preis geben.

Trotzdem geht es kaum verharmlosender und bei den aktuellen Diskussion so einseitig die Vorteile der Datenweitergabe an

Unternehmen darzustellen zeugt von Mut - oder einer gewissen Betriebsblindheit. Auf der anderen Seite ist es natürlich die Aufgabe eines wirtschaftsnahen Think-Tanks, den Verbrauchern die Weitergabe ihrer Daten schmackhaft zu machen.

Den Brief findet ihr komplett im CTRL-Blog. Um ein Interview wurde auch gebeten. Wir dürfen gespannt sein.

Geschrieben von Stefan in Datenschutz um 13:27

Kundendatei offen im Netz

Eintrag auf

Gilly's playground: Auf dem Server des Webshops New

Underwear fand sich per Google-Suche nach einer Adresse eine Kundenliste mit 837 Einträgen als .txt-Datei (nicht ausgeschlossen, dass das die komplette Kundendatei war). Selbst die unverschlüsselten Passwörter waren dort zu finden.

Auf eine Mail hin wurde die Datei schnell entfernt, auf eine Antwort auf die Mail wartet Gilly aber noch.

Wer dort jemals gekauft haben sollte, sollte besser das Passwort ändern (ebenso auf allen Seiten, auf denen das gleiche Passwort oder gar die gleiche Passwort-/Mailadressen-Kombination verwendet wurde). Wie auch bei dem Verlust von 56.000 Datensätzen bei PwC ein weiterer Grund, das gleiche Passwort nicht an mehreren Stellen zu verwenden.

Mehr auf Gilly's playground.

Geschrieben von Stefan in Datenschutz um 11:57

Neue Details zum Datenverlust bei PricewaterhouseCoopers

Golem.de und heise.de melden neue Details zum Datendiebstahl bei PricewaterhouseCoopers (PwC).

Offensichtlich sind unter den vermutlich 56.000 gestohlenen Datensätzen 12000 gmx.de-Mailadressen, 12.000 web.de-Adressen und jeweils zwischen 2200 bis 3300 Mailadressen von hotmail.de, t-online.de und yahoo.de. Laut golem.de kann PwC aber noch nicht abschließend sagen, wie viele Datensätze genau gestohlen wurden.

Die große Anzahl an Adressen beruht wohl darauf, dass PwC die Bewerberdaten (unrechtmäßig) auch aus den vergangenen Jahren gespeichert wurden. Pikanterweise wurden dabei die Passwörter nicht als Hash, sondern im Klartext gespeichert.

Mit den Mailadressen und Passwörtern wurde dann versucht, sich z.B. bei Click&Buy und Moneybookers anzumelden.

Um dem ganzen die Krone aufzusetzen hatten rund 2000 der Teilnehmer an einer Web-Umfrage teilgenommen, ob sie die

gleichen Passwörter an mehreren Stellen im Internet einsetzen. Rund 80% der Befragten sollen angegeben haben, dass sie ihr Passwort an mehreren Stellen verwenden. Rund 50% hätten das gleiche Passwort wie bei ihrem Mailaccount verwendet.

Na dann Prost Mahlzeit!

Geschrieben von Stefan in Datenschutz um 10:50

Google bewegt sich bei Speicherdauer von Suchanfragen

Wie golem.de und heise.de melden, hat Google angekündigt, die IP-Adressen aus der Internetsuche ab Ende September nur noch 9 Monate zu speichern. Nachdem sie anfänglich unbegrenzt gespeichert wurden, hatte Google im März 2007 bereits die Begrenzung der Speicherdauer auf 18 Monate angekündigt. Wie netzpolitik.org aber zurecht hervorhebt, handelt es sich dabei immer noch um eine 1,5-fache Vorratsdatenspeicherung (dort werden die IP-Adressen nur 6 Monate gespeichert).

Wie computerwelt.at meldet hat Google weiterhin angekündigt, die IP-Adressen, die bei der Nutzung von Google Suggest (d.h. die Suchbegriff-Vorschläge im Google-Suchfenster, in der Firefox-Suchbox oder der Google-Chrome-Adressleiste) anfallen, künftig nur noch 24 Stunden zu speichern.

Damit dürfte Google wohl auf den Druck der Datenschützer in Europa und den USA reagieren. Vermutlich dürfte auch der öffentliche Druck, der in den letzten Tagen nach der Veröffentlichung von Googles Browser Chrome aufgekommen ist, mitverantwortlich sein.

Geschrieben von Stefan in Datenschutz um 10:11

Montag, 8. September 2008

Kundendaten: Versuchte Erpressung der Telekom?

Der Focus meldet, dass ein ehemaliger Call-Center-Mitarbeiter soll versucht haben soll, die Telekom zu erpressen - angeblich, weil er keine andere Möglichkeit sah, auf ein Sicherheitsleck aufmerksam zu machen. Der ehemalige Mitarbeiter sei Ende August verhaftet worden, nachdem er per Mail von der Telekom 10.000 Euro gefordert habe und damit gedroht habe, andernfalls Datenlecks offen zu legen und Kundendaten an die Medien zu geben. Nach seiner Verhaftung sagte er, er habe vom Betreiber seines Call-Centers das Passwort für die interne Kundendatenbank "Cosma" der Telekom erhalten. Er habe schon 2007 erfolglos versucht, die Telekom auf die Sicherheitslücke aufmerksam zu machen, ihm sei aber kein Gehör geschenkt worden. Die Erpressung habe er dann angeblich in Absprache mit einem TV-Journalisten begonnen, um die Telekom zur Behebung des Lecks zu bewegen.

Geschrieben von Stefan in Datenschutz um 08:11

Lidl vor Bußgeldern in Millionenhöhe wegen Bespitzelung

Laut Spiegel Online blüht dem Discounter Lidl wegen der Ausspionierung von Mitarbeitern ein Bußgeld in (einstelliger) Millionenhöhe. Die Datenschutzbeauftragten mehrerer Länder wollen im September Bußgeldbescheide verschicken. Neben der bekannt gewordenen Bespitzelung von Mitarbeitern im Privatbereich werden auch die unzulässige Videoüberwachung sowie langfristige Datenspeicherung bestraft. Wirklich wundern kann auch nicht, dass auch Bußgelder wegen nicht bestellter Datenschutzbeauftragten verhängt werden.

Lidl soll angekündigt haben, das Bußgeld zu akzeptieren. Insofern scheint der Konzern aus dem verheerenden Medienecho und der (zumindest vorübergehenden) Kundenabwanderung gelernt zu haben und versucht das Thema in den Medien möglichst klein zu halten.

Geschrieben von Stefan in Datenschutz um 07:36

So macht man Werbung oder: Pro 7 als Subway-Haussender (Update 10.9.)

Stefan Niggemeier hatte vor einigen Wochen kritisiert, dass die Reality-Dokus und Wissenschaftssendungen auf Pro 7 den Eindruck erweckten, als wäre ihr Hauptzweck die Promotion irgendwelcher Franchise-Fastfoodketten. Pro 7 hatte auf seine Nachfrage natürlich erklärt, dass die Berichterstattung nur journalistische Gründe habe.

Nun legt Stefan Niggemeier mit einer Pressemeldung der PR-Agentur foleys nach, die tief blicken lässt.

Schon im letzten Jahr ist es foleys PR gelungen, SUBWAY® Sandwiches in bekannten TV-Formaten wie ?Galileo? oder ?Deine Chance ? 3 Bewerber, 1 Job? auf PRO7 zu platzieren. Auch in 2008 zeigt sich die Ulmer Agentur auf diesem Gebiet sehr erfolgreich...

Das Team von foleys PR initiierte und begleitete dabei alle Drehs, bereitete deren Inhalte vor, briefte die Protagonisten und TV-Teams und stand ihnen und den jeweiligen Franchisepartnern vor ORT mit Rat und Tat als verantwortliche Kontrollinstanz (und Pressesprecher) zur Seite. Das Resultat: Über 73 Minuten kostenlose TV-Präsenz

für SUBWAY® Sandwiches, mit 12,91 Millionen Gesamtschaltquote und einem Mediawert von über zwei Millionen Euro.

Die Offenheit, mit der die PR-Agentur ihre erfolgreiche Schleichwerbung anpreist, überrascht dann doch (die Medienaufsicht scheint ja wirklich als zahlos eingeschätzt zu werden). Insbesondere kommt die Frage auf, was Pro 7 davon hat. Da die Werbung laut foleys ja "kostenlos" war, scheiden finanzielle Gründe aus. Somit bleiben nur noch die Essvorlieben der zuständigen Redakteure - oder Pro 7 (und wie aus der ganzen Pressemeldung hervorgeht auch Kabel 1) hat wirklich große Probleme, die eigenen Formate mit Inhalt zu füllen und rennt jedem hinterher, der zwei Worte in ein Mikro stammeln kann.

foleys PR achtet dabei auf Ausgewogenheit: Nicht nur die Produkte der Sandwichmacher sollen dem deutschen Fernsehpublikum präsentiert werden. Die PR-Spezialisten legen auch Wert darauf, dass alle Facetten ihres Kunden gut beleuchtet werden.

Insbesondere das letzte Zitat stimmt mich froh. Über die Ausgewogenheit im deutschen Fernsehen müssen wir uns also keine Sorge machen - schließlich geht es nicht nur um die Produkte der Schleichwerber, nein auch die anderen Facetten werden "gut beleuchtet".

Man kann das natürlich auch noch weiterspinnen. Wenn sich so erfolgreich "Wissenschaftsmagazine" und Reality-Dokus mit Fastfood füllen lassen, wieso gehen wir nicht noch ein paar Schritte weiter? Die nächste Serie spielt bei McDonald's. Die Nachrichten füllen wir mit neuem Bratfett bei Burger King und kaltem Kaffee bei Starbucks. Das Wetter wird aus dem Pizza Hut um die Ecke präsentiert und die Hauptfiguren des Primetime-Spielfilms frühstücken bei Dunkin' Donuts (sollten sich weitere bekannte Fastfood-Ketten nun diskriminiert fühlen, bitte ich um Mitteilung an die Pro 7-Programmredaktion).

Ein Gerücht wird wohl bleiben, dass Pro 7 in Zukunft Pro Sub® heißen wird - auch wenn das wohl keinen mehr wirklich wundern würde...¹

¹ Die Diskussionen, ob Sub die Abkürzung für Subway oder Subventioniertes Programm sein soll, sind noch nicht abgeschlossen...

Update: Stefan Niggemeier hat weitere Details ausgegraben: Im Quelltext des Content Management Systems des Unternehmens fanden sich unveröffentlichte Details zur Platzierung von Subways-Werbung im Fernsehen. Mittlerweile hat sich auch die PR-Agentur foleys in den Kommentaren zu dem aktuellen Beitrag zu Wort gemeldet und fühlt sich mißverstanden und als Opfer einer Kampagne. Amüsant ist besonders dieser Ausschnitt des Kommentars: Wir haben uns auf unserer Website, die rein zur Eigenwerbung gegenüber Neukunden dient, auf welcher wir auch nie eine Pressemeldung veröffentlicht haben, evtl. missverständlich ausgedrückt. Diesen Satz von einer PR-Agentur finde ich bemerkenswert. Was ins Netz gestellt wird, kann natürlich auch von jedem gelesen werden - ob die Seite nur für potentielle Neukunden gedacht ist, oder nicht. Wenn man sich als PR-Agentur darüber beschwert, sollte man sich Gedanken über die Kompetenz der eigenen Kommunikationsfachleute machen...

Geschrieben von Stefan in Fernsehen um 06:29

Freitag, 5. September 2008

netzpolitik.org-Podcast mit Peter Schaar

Der aktuelle Podcast von netzpolitik.org ist ein ein zehnmütiges Interview mit dem Bundesdatenschutzbeauftragten Peter Schaar. Er äußert sich zu den Ergebnissen des "Datenschutzgipfels", der Aktualität des Datenschutzes und an welchen Stellen die Datenschützer in Zukunft noch Handlungsbedarf des Gesetzgebers sehen.

Das Interview gibt es mp3 und ogg auf netzpolitik.org.

Geschrieben von Stefan in Datenschutz um 15:29

Verfassungsgericht verlängert Eilentscheid zur Vorratsdatenspeicherung

Das Bundesverfassungsgericht hat seine im März getroffene Eilentscheidung, den Zugriff auf die durch die Änderung an den §§ 113a und 113b des Telekommunikationsgesetzes zu beschränken, um 6 Monate verlängert. Somit ist der Zugriff auf die Daten bis März 2009 weiterhin nur bei schweren Straftaten möglich. Gleichzeitig wurde der Bundesregierung auferlegt, im Januar 2009 eine weitere Statistik über die Nutzung der durch die Vorratsdatenspeicherung erhobenen Daten vorzulegen. Die erste Statistik, die Anfang September vorgelegt worden war, ist vom AK Vorratsdatenspeicherung, in dem sich 34.000 Menschen zur Klage zusammengeschlossen haben, scharf kritisiert worden.

Geschrieben von Stefan in Datenschutz um 07:07

Abschalten der eindeutigen ID von Googles Browser Chrome

Golem.de hat eine Anleitung veröffentlicht, wie man die eindeutige ID des Google Browsers Chrome abschalten kann. Offenbar muss nicht nur eine Datei editiert und schreibgeschützt werden. Findet der Browser die Datei Local State schreibgeschützt vor, erstellt er sie als Local State.tmp neu. Auch diese Datei muss dann dementsprechend editiert werden.

Die genaue Anleitung auf golem.de.

Geschrieben von Stefan in Datenschutz um 06:55

Donnerstag, 4. September 2008

Datenschutz-Gipfel: Bundesregierung will die Weitergabe von Adressaten von der Zustimmung Betroffener abhängig machen

Auf der Pressekonferenz nach dem sogenannten Datenschutz-Gipfel hat Innenminister Dr. Wolfgang Schäuble soeben bekannt gegeben, dass die Weitergabe von Adressen von der ausdrücklichen Zustimmung der Betroffenen abhängig gemacht werden soll. Damit wird die bisherige Praxis geändert, dass Adressdaten weitergegeben werden, wenn kein Widerspruch vorliegt. Dies wird aber wohl nicht die Daten betreffen, die ein Unternehmen selbst erhoben hat. Ein Gesetzentwurf soll bis Ende November vorliegen.

Außerdem soll die Umsetzung bestehender Gesetze verbessert werden. Weiterhin setzt die Konferenz der Innenminister der Länder eine Expertenkommission einsetzen, die die bestehenden Regelungen überprüfen sollen und unter anderem prüfen soll, ob Kundendaten nur noch verschlüsselt gespeichert werden sollten und jeder Zugriff auf Kundendaten protokolliert werden soll.

Es soll ein Datenschutz-Audit-Siegel geben, das Unternehmen bekommen können, die über die gesetzlich vorgeschriebenen Regelungen hinaus Maßnahmen für den Datenschutz getroffen werden. Diskutiert wird noch über die Stärkung der Datenschutzbeauftragten in Unternehmen und sowie Unternehmen zu verpflichten, Verletzungen des Datenschutzes öffentlich zu machen.

Update: Links eingefügt.

Geschrieben von Stefan in Datenschutz um 12:15

WISO verschickt wegen Datendiebstahls 56.000 Warn-E-mails

Die Redaktion des ZDF-Magazins WISO hat 56.000 E-mails verschickt, in die Empfänger davor gewarnt werden, dass man bei Recherchen zu einem Beitrag auf E-mail-Adresse und Passwort gestoßen sei. Die E-mail gibt die Mailadresse und das (gekürzte) Passwort an und fordert dazu auf, das Passwort überall dort zu ändern, wo es verwendet worden ist (im Datenschutz-Blog findet sich ein Screenshot der E-mail).

Zur Herkunft der Daten auf

Geschrieben von Stefan in Datenschutz um 11:15

Über absurde Züge bei der Kommentierung des Datenschutzes

Ich habe gerade eben den Kommentar von Burkhard Müller-Ullrich (einer der Autoren im Blog "Achse des Guten") im Tagesspiegel gelesen. Titel: Lasst die Daten frei - Die deutsche Angst vor Bespitzelung nimmt absurde Züge an.

Ich unterstelle dem Autor einfach mal, dass der Schluss des Kommentars, auf den sich auch die Überschrift bezieht, satirisch gemeint ist, wenn er schreibt:

Vielleicht liegt darin das einzige Gegenmittel zu der Gefahr, die von den Daten ausgeht: Lasst alle Daten frei. Lasst uns in Daten waten. Eine Datensintflut möge kommen und alle Lotto-Firmen, Nummerndiebe, Kontenknacker, Passworträuber und Trojaner sollen darin ersaufen.

Es kann eigentlich nur Satire sein, denn jeder, der auch nur ein wenig Ahnung von modernen Data-Mining-Methoden

hat, weiß dass mehr Daten letztlich nur eine bessere Vernetzung der Daten und bessere Erstellung von Nutzerprofilen bedeutet. Es mag zwar etwas länger dauern, bis das Profil vorliegt, mit den heutigen Methoden ist dies aber kontrollier- und optimierbar. Auch jeglicher andere Datenmißbrauch funktioniert mit einem Mehr an Daten im Regelfall besser. Daher muss man von Satire ausgehen, wenn man dem Autor nicht jegliche Kompetenz in Sachen Datenschutz absprechen will.

Was mir aber viel mehr aufstieß ist die Unterüberschrift "Die deutsche Angst vor Bespitzelung nimmt absurde Züge an" bzw. deren Begründung. Burkhard Müller-Ullrich hat kein Verständnis für die Sorge vor der Speicherung immer weiterer (biometrischer) Merkmale durch den Staat. Schließlich könne die Staatsverwaltung nur funktionieren, wenn der Staat seine Bürger identifizieren könne. Unklar bleibt aber, warum er dazu unbedingt biometrische Daten benötigen soll. Eine Identifizierung eines "normalen Bürgers" funktionierte in den letzten Jahren problemlos über den Personalausweis. Sicher haben sich die technischen Mittel verbessert (wenn auch weniger, als Sicherheitsexperten uns teilweise weiß machen wollen bzw. sich wünschen). Allein diese technischen Möglichkeiten bedingen aber noch keinen höheren Bedarf des Staates nach einer "besseren" Identifizierung.

Weiter heißt es:

Es gibt offenbar zwei Deutschlands. Das eine ist jener Überwachungsstaat, vor dem Datenschützer warnen und den kein liberal denkender Mensch akzeptieren kann. Das andere Deutschland lernt man kennen, wenn man sich auf eine Polizeiwache begibt, um eine Anzeige zu erstatten oder eine Zeugenaussage protokollieren zu lassen. Dann landet man in einer Art Zeitmaschine. Die Beamten kämpfen mit vorsintflutlichem Gerät, der Funksprechverkehr lässt sich so einfach abhören, dass er auch gleich als Radioprogramm gesendet werden könnte; und wenn ein Polizist ein Foto einer verdächtigen Person braucht, dann bekommt er es erst Stunden später von der zuständigen Meldebehörde per Fax, und zwar in Form eines schwarzen Kleckses.

Wenn man bei dem "anderen Deutschland" den Bezug zum Datenschutz vermisst, dürfte es wohl daran liegen, dass kein Bezug vorhanden ist. Denn was nützen neueste biometrische Methoden, wenn die Behörden mit völlig veralteter Technik arbeiten? Letztlich spricht genau diese mangelhafte Ausstattung noch eher für die Kritik an der Speicherung biometrischer Methoden, denn wo veraltete Technik waltet, sind oft Sicherheitslücken nicht weit.

Widersinnig wird der Kommentar, wenn man den Schluss auf die weiter oben geäußerten Thesen bezieht.

Das Herumliegenlassen von brisanten Daten scheint geradezu ein Signum unserer Epoche zu werden: hier ein Laptop mit militärischen Geheimnissen im unbewachten Auto, dort eine CD mit den Sozialversicherungsnummern von halb Großbritannien.

Wenn das nicht für eine Datensparsamkeit des Staates spricht, was dann? Daten, die nicht gespeichert sind, können nicht verloren gehen. Da im Moment noch nahezu alle Fingerabdruckscanner mit geringem Aufwand überlistet werden können (siehe z.B. hier und hier), ergeben sich ganz neue Gefahren wenn biometrische Daten verloren gehen.

Es empfiehlt sich, den Beitrag von Gerhart Baum (Ex-Innenminister und an einigen Verfassungsklagen zur staatlichen Datenspeicherung beteiligt) auf Spiegel Online zu lesen. Er zeigt auf, warum der Staat aktiv gegen den Datenhandel werden muss - und seine eigene, seit den Anschlägen vom September 2001 hochgefahrene Sammelwut einschränken muss.

Geschrieben von Stefan in Meinung um 08:03

Mittwoch, 3. September 2008

Googles Browser Chrome - Open Source oder nicht?

Im Moment gibt es unterschiedliche Ansichten darüber, ob Googles neuer Browser Chrome Open Source ist oder nicht. Wäre der Quelltext offen gelegt, ließe sich sehr schnell klären, ob und wenn ja in welchem Maße der Browser Daten "nach Hause funkt".

Laut dem Datenschutz-Blog (mit Link auf Punkt 10.2 der Nutzungsbedingungen von Chrome) und Standart Tolleranz Maschine handelt es sich bei Chrome selbst nicht um Open Source. Allerdings gibt es wohl das Open Source Projekt Chromium, auf dem Chrome basiert. Diese ähnliche Namensgebung scheint für viel Verwirrung zu sorgen.

Auch wenn in den in den Kommentaren zu den Blog-Einträgen sowie in anderen Blogs Gegenteiliges gesagt wird, ist Googles Browser Chrome wohl kein Open Source. Offensichtlich haben viele die Google-Ankündigung ohne Hinterfragen übernommen.

Bis die Frage, inwieweit Chrome "nach Hause telefoniert" endgültig (z.B. mit Netzwerk-Sniffen wie Wireshark) geklärt ist (sollte Google nicht doch noch den Quellcode freigeben), wird es wohl noch etwas dauern.

Geschrieben von Stefan in Datenschutz um 19:40

Blog wirft Telekom illegale Herausgabe von Verbindungsdaten vor

Das Blog daten-speicherung.de wirft der Deutschen Telekom AG die illegale Herausgabe von Verbindungsdaten vor. Diese dürfen nur nach richterlicher Anordnung herausgegeben werden. Die Telekom nach einer von dem Blog anonymisiert vorgelegten PDF-Datei die Daten aber in einer Art von vorausseilendem Gehorsam auf eine Anfrage der Staatsanwaltschaft herausgegeben, bei der es nur um die Ermittlung des Anschlussinhabers einer IP-Adresse ging.

Die Daten gingen dazu noch nur äußerst dürftig geschützt per Mail durchs Netz: als passwortgeschützte Zip-Datei - das Passwort war ein vierstelliges Wort, offensichtlich in jedem Wörterbuch auffindbar und somit in kürzester Zeit knackbar.

Ausführlich auf daten-speicherung.de.

Geschrieben von Stefan in Datenschutz um 19:00

EU will größte Fingerabdruckdatenbank der Welt aufbauen

Das Europaparlament hat heute den biometrischen Kontrollen im Rahmen des Visa-Informationssystems [VIS] zugestimmt.

Damit müssen ab 2009 alle aus visumpflichtigen Staaten Einreisende ihre Fingerabdrücke abgeben, allerdings kann zu Stoßzeiten auch nur stichprobenartig kontrolliert werden. Es wird dann geprüft, ob die Fingerabdrücke mit den im Visum angegebenen übereinstimmen. Die genommen Fingerabdrücke werden 5 Jahre lang gespeichert. Binnen 10 Jahren soll so die größte Fingerabdruckdatenbank der Welt entstehen.

Via dem Virtuellen Datenschutzbüro und ORF Futurezone.

Geschrieben von Stefan in Datenschutz um 18:34

Monatsbrennpunkt des BSI: RFID

Der Brennpunkt des Bundesamts für Sicherheit in der Informationstechnik (BSI) befasst sich in diesem Monat mit RFID, der "Radio Frequency Identification".

Im Brennpunkt finden sich Informationen zur Geschichte, zum Einsatz sowie zu Chancen und Risiken der RFID-Technologie, unter anderem auch im ePass.

Wer sich informieren will, findet den Schwerpunkt hier.

Geschrieben von Stefan in Datenschutz um 14:26

Googles Browser Chrome - neuer Browser mit individueller ID (Update 8.9.)

Googles neuer Browser Chrome ist im Moment ja in aller Munde. Gestern veröffentlicht beherrscht der auf der Safari-Engine Webkit basierende Browser heute alle Technikseiten der Zeitungen und Onlinemagazine.

Oft stehen nicht nur die Features wie die von Google angepriesene Schnelligkeit, die in einzelnen Prozessen

gestarteten Tabs oder der "Inkognito-Modus". Direkt wurden Warnungen vor der Marktmacht Googles laut. Sicherlich, der Browser allein

macht es nicht. Die Marktmacht Googles ergibt sich vor allem aus dem Suchmaschinengeschäft (für Deutschland gehen die

meisten Seiten von einem Marktanteil von mindestens 90% aus) - und der vielen Felder, in denen Google mittlerweile aktiv

ist. Google Mail als Freemailprovider, Google Text und Tabellen, die Google Desktop-Suche, das in den USA bereits gestartete Google Health (Gesundheitsdaten/-akten) bei Google hinterlegen, Google Maps/Earth, YouTube, usw.

Der entscheidende Punkt dürfte sein, nicht zu vergessen dass es sich bei Google um ein gewinnorientiertes Unternehmen

handelt. Dann muss man sich die Frage stellen, warum Google einen Browser herausbringt. Sicher nicht aus philanthropischen Motiven, sondern um etwas zu erreichen. Die meisten Kommentatoren vermuten, dass Googles Browser vor

allem als Angriff auf Microsoft zu verstehen ist. Die Überlegung ist zumindest naheliegend, schließlich hat Microsoft immer noch mit deutlichem Abstand den höchsten Marktanteil bei den Browsern (man könnte es auch als eine Art Retourkutsche verstehen: Microsoft versuchte erfolglos Yahoo zu übernehmen, ein Angriff auf Googles Kerngeschäft der

Internetsuche. Nun geht Google auf den Internet Explorer los. Sicherlich ist Chrome schon länger in Entwicklung.

Reizvoll ist der Gedanke aber trotzdem...). Einige vermuten sogar, dass Chrome auf lange

Sicht die Betriebssysteme attackieren soll, indem nach und nach immer mehr der Google-Applikationen wie Google Text und

Tabellen auch offline eingebunden werden sollen.

Golem.de meldet

mittlerweile, dass jeder installierte Chrome eine eigene, einzigartige ID bekommt. Diese lässt sich zwar deaktivieren, aber wie viele Menschen werden das tun? Wie viele werden überhaupt etwas von dieser ID erfahren?

Praktisch - für Google - denn so lassen sich alle Benutzeraktionen, Sucheingaben, die Suchervollständigkeit usw. immer

auf einen Benutzer zurückführen. Hat man bei der "normalen" Suche noch das Problem wechselnder IPs, mit Chrome wird

Googles Traum wahr. Wer Werbung möglichst personenbezogen einblenden will, kann normalerweise von solch einer Fülle

von Daten nur träumen...

Es sollte sich also jeder gut überlegen, ob er/sie Chrome installiert. Das mindeste sollte sein, die Anmerkung zum Datenschutz durchzulesen.

P.S. Wie es es bei einem neuen Browser fast nicht anders zu erwarten ist, wurden die ersten Schwachstellen laut heise.de auch schon in Chrome gefunden.

Update 8. September 2008: Mittlerweile meldet heise.de erste Exploits für die Sicherheitslücke. Ein weiterer

Artikel widmet sich dem Thema Datenschutz und Google Chrome.

Auch ein Sprecher des Bundesamtes für Sicherheit in der Informationstechnik hat vor Chrome gewarnt, aus Datenschutzgründen und da viele Menschen den Beta-Status der Software nicht erkennen würden.

Geschrieben von Stefan in Datenschutz um 13:20

Bundesdatenschutzbeauftragter kritisiert Datenhandel der Meldebehörden

In einem Interview in der Westdeutschen Allgemeinen Zeitung hat der Bundesdatenschutzbeauftragte Peter Schaar die Praxis von Meldeämtern kritisiert, die Meldedaten an Firmen zu verkaufen.

Dies sei besonders problematisch, da die Daten zwangsweise erhoben werden. Außerdem würden von den Unternehmen nicht nur die Adressen von Schuldnern erhoben, sondern oftmals die gesamten Adressbestände abgefragt, weitergegeben und bei den Firmen selbst gespeichert und gesammelt. Peter Schaar forderte mindestens ein allgemeines Widerspruchsrecht der Bürger. Dieses gebe es zur Zeit nur in Ausnahmefällen, z.B. bei Bedrohung.

Peter Schaar wiederholte auch seine Forderung nach Änderung der gesetzlichen Regelungen, so dass die Verbraucher der Weitergabe ihrer Daten aktiv zustimmen müssten.

Peter Schaar erhofft sich vom morgigen "Datenschutz-Gipfel" mit Innenminister Schäuble konkrete Verbesserungen für den Datenschutz.

Das komplette Interview findet sich hier im Onlineauftritt der WAZ.

Geschrieben von Stefan in Datenschutz um 13:05

Dienstag, 2. September 2008

Von der Schwierigkeit, ein Geheimnis zu bewahren

Gerade eben lese ich auf Spiegel Online mal wieder so einen Artikel, der nur Kopfschütteln hervorrufen kann.

Ein großes "Meinungsblatt" mit 4 Buchstaben konnte es nicht lassen, trotz Nachrichtensperre Details über die Todesumstände der in Leipzig entführten Michelle zu veröffentlichen.

Natürlich, es ist die Aufgabe von Journalisten, über Dinge zu berichten. Oft ist es auch notwendig, über Dinge zu berichten, die noch nicht bekannt sind oder von gewissen Kreisen als geheim angesehen werden (man denke an die BND-Abhörskandale). Aber jeder Journalist sollte auch moralische Grenzen haben. In diesem Fall hat die Nachrichtensperre ja gute Gründe, man möchte kein "Täterwissen" preis geben, um so bessere Chancen zu haben, den Täter zu ermitteln. Gerade bei Fällen von entführten Kindern, die vielen Leuten (noch?) nahe gehen, sollte man sich beherrschen können.

Aber auch hier scheint der Druck für einige wenige zu groß zu sein - der Druck, andere könnten schneller sein und anstelle einem selbst "15 Minuten Ruhm" ernten...

Geschrieben von Stefan in Meinung um 10:20