planet ccc - blogs and more around ccc, ccc-hamburg and attraktor

July 10, 2014

Netzpolitik.org

Die Internetversteher im Taka-Tuka-Land: "Nur weil man etwas nicht sieht bedeutet das noch nicht, dass es nicht da ist"

Dieser Gastbeitrag ist von Joachim Bellé, Aktivist im Arbeitskreis gegen Internet-Sperren und Zensur (AK Zensur).

An Pippi Langstrumpf muss ich immer denken, wenn jemand mit großer Stärke, ungeachtet der Physik und Logik naive Gedanken durchzieht und sich die Welt ohne Rücksicht auf Andere so macht, wie sie einem gefällt. Selbst Kinder verstehen Pips Welt und können sich, wohl wissend, dass alles nur Phantasie ist, totlachen. Erwachsene verlieren offenbar diese Fähigkeit. Mit verbissenem Ernst und der Macht der Gesetze längst vergangener Zeiten biegen sie sich die Welt, wie sie nicht sein sollte.

Was ist geschehen? Die Bundesprüfstelle für Jugendgefährdende Medien (BPjM) stellt Strafanzeige gegen die Hacker, die ihre indizierte Liste zum Internet veröffentlicht haben. Sie droht, ungeachtet der Pressefreiheit, der mit 500.000 Euro Bußgeld, wer in Artikeln zum Thema auf eine Seiten verlinkt, die (keine) Links zu indizierten Inhalten führt. Natürlich, da stehen da auf der verlinkten Webseite Adressen im Klartext. Die sind aber nicht anklickbar. Die stehen nicht da, um sich Porn reinzuziehen. Die stehen da, um einen Missstand aufzuzeigen.

Verboten

Ohne Zweifel ist es verboten, die Liste der jugendgefährdenden Medien abzudrucken oder zu veröffentlichen. Wie absolut ein Gebot oder Verbot ist, das zeigt uns aber die BPjM selbst. Denn obwohl eine Zensur nicht statt findet, zensiert die Prüfstelle Medien. Das ist ihre Aufgabe. Es dürfte klar sein, das ist ein Widerspruch, der nur gerechtfertigt ist, wenn man die Verhältnismäßigkeit berücksichtigt. Manchmal ist eben die Missachtung von Verboten zum Wohle Aller absolut geboten.

Die Frage nach dem Warum

Ist das hier bei dem Leak der Indexliste der Fall? Warum taten sie das? Ich kann das nicht sagen. Doch ich kann sagen, warum ich das getan hätte.

So 2009 wolle Ursula von der Leyen Stopp-Schilder im Internet installieren. Wer auf böse Inhalte im Netz zugreifen wollte, der sollte statt der Inhalte ein Stopp-Schild sehen. Damals ging es um Bilder von Kindesmissbrauch. Doch Einige forderten durchaus auch die Webseiten auf der Indexliste der BPjM zu sperren. Wir fanden das alles falsch. Ein Grund dafür war, dass wir die Sperrlisten anderer Länder einsehen konnten. Wir konnten uns davon überzeugen, dass Seiten zu Unrecht gesperrt wurden und das vorgegebene Ziel offenbar nur eine untergeordnete Rolle spielte. Diese Listen hatten immer eine sehr mangelhafte Qualität. Wenn politische Parteien gesperrt wurden, dann muss man von Missbrauch und undemokratischem Verhalten sprechen.

Ursula von der Leyen konnte sich nicht durchsetzen. Das hat dazu geführt, dass heute 97% der den Behörden bekannten Seiten mit Missbrauchsbildern von den Hostern selbst vom Netz genommen werden. 97% Erfolg durch Löschen stehen gegen 0% Entfernung der Bilder durch Sperren. Löschen statt Sperren ist Realität geworden, auch weil Listen indizierter Seiten veröffentlicht wurden.

Diese Geschichte lässt mich an den 1934 im KZ in Oranienburg gestorbenen Erich Mühsam denken. Der dichtete und starb im vollem Bewusstsein um die Konsequenzen: „Brich das Gesetz".

Leak?

Man kann die Frage stellen, ob es sich bei dem Leak überhaupt um die Veröffentlichung der indizierten Liste handelt. Zunächst einmal haben die Hacker klar eine Liste von nicht besonders tollen Webseiten veröffentlicht. Es ist zwar technisch etwas komplizierter, doch diese Liste kann sich jeder selbst erstellen. Man braucht dazu eine beliebige Liste von Webseiten aus dem Netz und eine FritzBox. Listen mit Millionen von URLs findet man zum Beispiel bei Alexa. Bei der FritzBox stellt man den Jugendschutzfilter ein und dann wirft man die Liste dagegen. Überall, wo die FritzBox den Zugang verweigert steht die Seite auf dem Index. Sie sollten auf keinen Fall in einem Forum im Internet nachfragen, warum die FritzBox eine Seite www.bösexxx.de sperrt. Sie veröffentlichen damit einen Teil der indizierten Liste der BPjM. Sie dürfen sich auch nicht überzeugen, ob diese URL wirklich böse ist. Denn einige Einträge auf der Liste beinhalten Webadressen, deren bloßes Ansehen laut BPjM Strafverfolgung nach sich ziehen kann. Vermutlich bekommen sie auch Beulenpest davon. Vermutlich ist es besser ganz auf das Netz zu verzichten um ganz sicher zu sein. So muss man jedenfalls die Aussage der BPjM interpretieren.

Wobei sich gleich die Frage stellt, woher die Behörden denn wissen wollen, welche Seite ich denn gerade aufgerufen habe. Entweder möchte uns die BPjM Angst machen oder die Zusammenarbeit der NSA mit den deutschen Geheimdiensten ist noch fataler, als sowieso gedacht. In diesem Kontext ist die Aussage der BPjM schon als recht zweifelhaft. Wer mit dem „Lauschern an der Wand", Angst und

Drohungen argumentiert, dem soll ich vertrauen, dass er Grundrechte interpretieren und einschränken darf?

Ja, gegen Missbrauch und menschenunwürdige Inhalte im Netz muss vorgegangen werden. Die Sicht der Politik auf das Netz, die geistige Gleichschaltung der Medien, macht das jedoch unmöglich. Internet ist kein Radio und keine Zeitung.

Ist gleich gleich gleich?

Aber war das nun ein Leak der Liste? Das hängt davon ab, ob Gleichheit Identität bedeutet. Ich bin nicht mein Zwilling, obwohl wir gleich aussehen. Die veröffentlichte Liste ist keine Kopie der Liste der BPjM. Die ist nur das Ergebnis einer FritzBox Simulation. Sie ist nicht einmal 100% identisch.

Wer nun meint, das sei spitzfindig, der hat vielleicht Recht. Doch als Internetbürger muss man sehen, dass ich es mit Computern zu tun habe. Da spielt der Unterschied zwischen Gleichheit und Identität eine wesentliche Rolle. Man könnte (zugegeben sehr überheblich) sagen, als „Internetversteher“ ist mir das in Fleisch und Blut übergegangen.

Fakt ist in jedem Fall: es wurde nicht die Liste der BPjM veröffentlicht. Es wurde auch keine Kopie veröffentlicht. Die Hacker können nichts dafür, dass die BPjM auf ein Verfahren setzt, das man Security by Obscurity nennt. Die BPjM macht einen fatalen Fehler, veröffentlicht den Index und sucht nun einen Schuldigen.

Es ist Internet. Das lässt sich nicht so behandeln, wie der Playboy oder die Titanic. Man kann nicht einfach eine Auflage einer Zeitung einfach einkassieren. Man kann sich nicht die Welt nach Belieben und gegen jede Logik so machen, wie sie einem gefällt.

Piraten

Betrachtet man die von der BPjM verwendete Technik, so wird es auch für den Laien interessant. Die Liste beinhaltet die Webadressen nicht im Klartext. Statt dessen werden geschickte Prüfsummen veröffentlicht. Die wird vom „Jugendschutzprogramm“ oder von der FritzBox mit der Prüfsumme der Adresse verglichen, die ein Nutzer gerade ansehen will. Sind die Prüfsummen gleich, so wird der Zugang verweigert.

Der Vorteil: Man kann so eine Prüfsumme nicht einfach in den Browser eingeben um zu einer verbotenen Seite zu gelangen. So denkt die BPjM, die Liste sei ausreichend geheim.

Leider stimmt das so schon lange nicht mehr. Das Bittorrent Verfahren zum Tauschen von Dateien im Netz macht genau das Selbe. Ein Torrent ist im Wesentlichem eine solche Prüfsumme. Allerdings wird genau damit der Zugang ermöglicht statt, wie von der BPjM erwünscht, unterbunden. Das identische Verfahren mit umgekehrtem Ergebnis? Vielleicht hätte man vorher ein wenig nachdenken können.

Wenn the PirateBay Urheberrechtsverletzungen begeht, indem es Prüfsummen von Medien veröffentlicht und damit diese Medien zugänglich macht, dann hat die BPjM mit ihrer indizierten Liste von Prüfsummen die verbotenen Inhalte ebenfalls zugänglich gemacht. Nur weil jemand den Hashcode noch nicht lesen kann bedeutet das noch lange nicht, dass niemand ihn lesen kann. Nur weil man etwas nicht sieht bedeutet das noch nicht, dass es nicht da ist. Das haben die Hacker eindrucksvoll bewiesen.

Die Quelle der Liste ist ganz eindeutig die BPjM selbst. Und die hat diese Liste persönlich und ungefragt in der Welt verteilt, grob fahrlässig und ganz ungeachtet der Konsequenzen, in dem Wissen, das bisher keine Sperrliste unveröffentlicht bleib. Daran ist nichts überraschend. Das ist nur logische Konsequenz aus dem Versuch das Netz zu zensieren statt den Menschen den Umgang mit dem Netz beizubringen.

Wie Pippi Langstrumpf machten sie sich die Welt, wie es ihnen gefällt. Die Piraten, die „Hacker“ sind schuldig. Die BPjM macht technisch genau das Selbe und ist unschuldig.

Qualität

Die Qualität der Liste der BPjM ist schnell besprochen. Über die Hälfte der Prüfsummen verweisen auf Seiten schon lange nicht mehr existieren. Unter den verbotenen Seiten befinden sich welche, die in Europa gehostet werden. 37 Seiten aus Deutschland wurden indiziert, obwohl das nach den Aussagen der BPjM und der Bundesregierung weder notwendig noch angemessen ist. Viele Seiten verweisen auf legale Dinge, etwa Internet-Shops. Viele Seiten benötigen einen Login und stellen damit eine geschlossene Gruppe da. In geschlossenen Gruppen darf legal auch harte Pornographie verbreitet werden. Viele Seiten verweisen auf Klickstrecken mit angeblich “aufreizenden Bildern” und ohne Effektiven Inhalt. Da kann man sich totklicken. Jeder Klick generiert Geld für die Betreiber für Nichts. Wer dadurch nicht geheilt wird auf jeden Mist zu klicken, dem ist nicht mehr zu helfen.

Viele Seiten sind nach US-Recht legal. Nur „Kinderpornographie“ habe ich nicht gefunden. Man sehe mir das nach. Braucht man eine Minute, um eine Seite zu prüfen, so braucht man 50h und keine Sekunde Pause, wenn man alles prüfen möchte. Die Chance, bei einer zufällig ausgewählten Seite auf der Liste auf sogenannte „Kinderpornographie“ zu stoßen, liegt im Promillebereich.

Wer behauptet, diese unverschlüsselte Liste würde den Zugang zu „Kinderpornographie“ ermöglichen, der kann nicht rechnen. Der hält sich eben für Pippi Langstrumpf, sehr süß, aber leider nicht realistisch. Internet ist offenbar Taka-Tuka-Land, ist Neuland. Und, um ein Zitat des Herrn Uhl einmal zu erweitern, nicht nur die USA verhält sich wie digitale Besatzer.

0

by Gastbeitrag at July 10, 2014 06:49 PM

US-Netzunternehmen und Start-Ups positionieren sich pro Netzneutralität

In der US-Debatte um Netzneutralität mischen immer mehr bekannte Netz-Unternehmen mit. Das ist etwas, was uns in Deutschland leider fehlt. Wie bereichernd wäre die Debatte hierzulande, vor allem im Hinblick auf die nahende Entscheidung im EU-Ministerrat, wenn sich bekannte Start-Ups und Web-Unternehmen für ein offenes Netz zu Wort melden würden, wie man das gerade in den USA beobachten kann?

Der Gründer und CEO von Kickstarter, Yancey Strickler, kommentiert in der Washington Post die Gefahr von Überholspuren im Netz: FCC's 'fast lane' Internet plan threatens free exchange of ideas.

> One thing we didn't have to worry about: access to the Internet. We didn't have to negotiate a deal with a cable company or other Internet service provider (ISP). We didn't have to hire lawyers to appeal to the Federal Communications Commission when we were offered an unfair price. We didn't have to worry about whether our site's content would be slower than a competitor that had some kind of exclusive "fast lane" deal. Such roadblocks would have created enormous logistical and financial hurdles — ones so big they might have shut us down before we got started.

Im Kickstarter-Blog ergänzt er: Supporting an Open Internet.

> It's easy to get lost in the minutiae and cynicism of the Net Neutrality debate. It's everything we hate about politics: money trumping common sense, and the loudest voices being those with the cash to hire lobbyists. Unfortunately, just believing in the common good rarely translates into political influence. But sometimes it does — as we saw with the SOPA victory in 2012, our voices can be powerful when we use them together. [...] The Internet as we know it depends on an open Web with equal access for all. That core principle is very much in doubt. Please join us in making a stand — for everyone's sake. Thanks

Althea Erickson, director of public policy, beim Handarbeits-Marktplatz etsy.com kommentiert im Firmenblog: Join Etsy in Fighting for an Open Internet.

> We spend considerable resources ensuring that large, high-resolution photos load quickly and efficiently. We have also considered offering our sellers the ability to create and share videos, which they could use to introduce themselves and the unique process behind their products. But our low margins would not allow us to pay for priority access to ensure our site loaded as quickly as rival sites if the FCC's proposed rules went into effect. If a consumer were to click on an Etsy shop and perceive delays in images loading or videos buffering, they would likely click away to another site, and our seller would lose that sale. We can't predict the future of e-commerce or product innovations, but we want to ensure that Etsy sellers can reach buyers with the same technologies as any other online retailer.

Sowas brauchen wir auch in Deutschland! Auf EU-Ebene entscheidet sich in den kommenden Monaten, ob der EU-Ministerrat sich auch den Empfehlungen des EU-Parlaments aus dem Frühjahr anschließt und sogenannte "Specialized Servcies", die angesprochenen Überholspuren gegen Geld, stark reguliert. Oder ob sich bei den intransparenten Verhandlungen im EU-Rat die Positionen der Telekommunikationsunternehmen durchsetzen, die in der Regel den besseren Zugang zu den einzelnen Regierungen haben. Es ist z.B. immer noch unklar, wie sich Deutschland dort positioniert. Wichtig ist, dass diese Debatte geführt wird und sich auch diejenigen zu Wort melden, deren Geschäftsmodelle bisher massiv von einem offenen Netz profitiert haben.

0

by Markus Beckedahl at July 10, 2014 05:27 PM

Einen Diplomaten ausweisen? Wie niedlich.

Kai Biermann kommentiert bei ZEIT-Online die Ausweisung eines US-Geheimdienst-Mitarbeiters: Einen Diplomaten ausweisen? Wie niedlich.

> Im Englischen gibt es eine Redewendung für dieses Verhalten: There is an elephant in the room – ein Elefant steht mitten im Zimmer, heißt es, wenn niemand das offensichtliche Problem ansprechen will und alle so tun, als sei es nicht vorhanden. Der Elefant NSA steht mitten in den bundesdeutschen Wohn- und Schlafzimmern, und niemand in der Bundesregierung will darüber reden.

Denn die Bundesregierung will lieber am NSA-System beteiligt sein:

> Die Bundesregierung profitiert davon, dass die NSA keine Grenzen und keine Gesetze achtet. Sie macht sich die Hände nicht schmutzig und bekommt trotzdem etwas von der Beute. Das Opfer sind dabei leider die Bürger – ihre Wähler.

0

by Markus Beckedahl at July 10, 2014 04:43 PM

Datenschutzbeauftragter in Schleswig-Holstein: Piraten verhindern Wiederwahl von Thilo Weichert (Update)

Bekommt (vorerst) keine dritte Amtszeit: Thilo Weichert.

Dr. Thilo Weichert dürfte regelmäßigen Leser/innen bekannt sein. Der Jurist und Gastblogger ist einer der kritischsten und aktivsten Datenschutzbeauftragten in Deutschland. Gerade sollte er im Landtag Schleswig-Holstein zum dritten Mal gewählt werden – was er jedoch mit einer Stimme verpasste:

> Die Wiederwahl des schleswig-holsteinischen Datenschutzbeauftragten Thilo Weichert ist am Donnerstag überraschend gescheitert. Für Weichert stimmten in geheimer Wahl nur 34 Landtagsabgeordnete. Damit fehlte ihm eine Stimme, um für fünf weitere Jahre im Amt bestätigt zu werden.

Die Regierung im Landtag SH hat 35 Sitze: SPD (22), Bündnis 90/Die Grünen (10) und SSW (3). Also fehlt mindestens eine Stimme der Regierungskoalition.

Gegen Weichert haben aber auch die sechs Piraten gestimmt. Das bestätigte der Piraten-Abgeordneter Patrick Breyer gegenüber netzpolitik.org. Ihre Kritik ist eine "Lex Weichert", welche die Kieler Nachrichten so beschreiben:

> Erst im Juni hatte das Parlament eine umstrittene Änderung des Datenschutzgesetzes verabschiedet, die die Amtszeitbegrenzung des Datenschutzbeauftragten aufhob. Ohne die Neuregelung hätte Weichert am Donnerstag überhaupt nicht mehr kandidieren dürfen.

Die Piraten schrieben schon im Februar in in einer Pressemitteilung:

> Dieser Antrag ist nach einhelliger Meinung der Piratenfraktion abzulehnen. Es muss keine 'Lex Weichert' geschaffen werden. Thilo Weichert hat in der Vergangenheit sehr viel für den Datenschutz nicht nur in Schleswig-Holstein, sondern auch weit darüber hinaus getan. Dafür danke ich ihm persönlich von ganzen Herzen. Unabhängig von der Person Thilo Weichert gibt es aber gute Gründe, weshalb der Landesdatenschutzbeauftragte maximal einmalig wiedergewählt werden sollte. So wird seine Unabhängigkeit insbesondere dadurch sichergestellt, dass er nicht bei der jeweiligen Landesregierung lieb Kind machen muss. Nötige harte Kritik an der Datenschutzpolitik der Regierung fällt leichter, wenn nicht die mögliche eigene Wiederwahl ansteht.

Die Piraten haben im Januar einen eigenen Gesetzentwurf zur offenen Ausschreibung des Amtes vorgelegt. Das derzeitige Verfahren halten sie für nicht tragbar.

Damit haben die Piraten mit dem Datenschützer Patrick Breyer die Wiederwahl des engagierten Datenschutzbeauftragten Thilo Weichert verhindert.

Wie geht es jetzt weiter? Nochmal Kieler Nachrichten:

> Nach Angaben von Landtagssprecher Tobias Rischer ist aber kein zweiter Wahlgang vorgesehen. Ein erneuter Versuch wäre somit erst im September möglich – nach der Sommerpause des Plenums. Weichert bleibt automatisch im Amt, bis ein neuer Datenschutzbeauftragter gewählt ist.

Ob die Regierungsfraktionen Thilo Weichert nochmal vorschlagen werden, ist derzeit noch nicht klar. Patrick Breyer würde es ihm nicht empfehlen.

Update: NDR 1 Welle Nord hat ein Zitat von Weichert:

> Ich habe nicht den Eindruck, dass ich auf die Nase gefallen bin. Das ich nicht gewählt worden bin, das habe ich zur Kenntnis genommen und alles Weitere kann ich im Augenblick gar nicht kommentieren, weil ich jetzt mit den Fraktionen keine Gespräche geführt habe. Dass ich nicht unbedingt immer ein angenehmer Datenschützer war, das ist allgemein bekannt. Dass ich ein qualifizierter Datenschützer bin, das hoffe ich, dass das die meisten zur Kenntnis genommen haben und das sollte eigentlich den Ausschlag geben.

0

by Andre Meister at July 10, 2014 04:08 PM

Großbritannien will "Notfallgesetz" zur Vorratsdatenspeicherung einführen

Die britische Regierung will schon nächste Woche in einem Eilverfahren ein Gesetz zur Vorratsdatenspeicherung beschließen. Der "Data Retention and Investigation Powers (DRIP) Act" ist eine Reaktion darauf, dass die bestehende EU-Richtlinie zur Vorratsdatenspeicherung im April durch den Europäischen Gerichtshof gekippt wurde. Das neue Gesetz ist ein Alleingang Großbritanniens, um Telefon- und Internetanbieter weiter zu zwingen, die Vorratsdaten ihrer Kunden zu speichern. Einen solchen nationalen Alleingang dürfte es nach der EuGH-Rechtsprechung eigentlich nicht mehr geben.

Der Gesetzentwurf wird laut BBC sowohl von der Regierungskoalition (Tories und Liberals) als auch der Labour Partei mitgetragen. Das Gesetz soll bis 2016 befristet sein und in einem Eilverfahren beschlossen werden. Premierminister Cameron (Tories) und Vize-Premier Clegg (Liberals) betrachten das Gesetz als notwendig, weil die Unternehmen sonst die bereits gespeicherten Vorratsdaten löschen könnten.

Jim Killock, Direktor der britischen NGO Open Rights Group, sagte dazu:

> **Die Regierung gibt damit stillschweigend zu, dass die aktuellen Gesetze zur zur Vorratsdatenspeicherung ungültig sind** [...]. Der Europäische Gerichtshof hat geurteilt, dass die Vorratsdatenspeicherung klar begrenzt sein muss und anlasslose Speicherung nicht gerechtfertigt ist [...].

Seit dem EuGH-Urteil sollen über 1.500 Menschen ihre Internetanbieter aufgefordert haben, keine Vorratsdaten mehr zu speichern, weil es keine EU-Rechtsgrundlage mehr gebe. Die Richtlinie verstieß laut EuGH gegen Grundrechte, und die gelten bekanntlich auf allen Ebenen. Deshalb sagen Experten, dass damit auch die nationalen Gesetze, die zur Umsetzung der EU-Richtlinie verabschiedet wurden, ungültig sind. Diese Auffassung ist aber umstritten. Die Unternehmen fürchten anscheinend dennoch, nun verklagt zu werden, wenn sie weiter Vorratsdaten speichern.

Die Britische Regierung behauptet dagegen, dass die Vorratsdaten auf keinen Fall gelöscht werden dürfen, weil das Ermittlungsprozesse und die Aufklärung von Verbrechen behindere, wie sie in einer Erklärung mitteilte. Diese Begründung ist keinesfalls überraschend: Unter allen 28 Mitgliedsstaaten der EU war Großbritannien schon immer der “Vorreiter” in Sachen Vorratsdatenspeicherung und setzte sich stets für die umfassendsten Regelungen ein.

Ausweitung statt Einstampfung?

Der Entwurf des Notfallgesetzes soll sogar eine Ausweitung der Vorratsdatenspeicherung vorsehen, auch wenn die Regierung offiziell das Gegenteil ankündigt. Zum einen soll die Regelung nun auch explizit für ausländische Unternehmen gelten, zum anderen könnten nun auch weitere Daten, die über reine Metadaten hinausgehen, betroffen sein. Das legen Formulierungsänderungen im Gesetz nahe, die GIGAOM herausgearbeitet hat.

Das die neue Regelung nun, drei Monate nach dem EuGH-Urteil, in einem Eilverfahren beschlossen werden soll, macht auf jeden Fall stutzig. Die britische Innenministerin Theresa May soll in dem Zusammenhang sogar gesagt haben, dass es bei dem neuen Gesetz um Leben und Tod gehe. Wenn derartige PR-Geschütze aufgefahren werden, muss es der britischen Regierung wirklich wichtig sein, die Vorratsdatenspeicherung wieder einzuführen. Man fragt sich nur warum eigentlich, wo doch der britische Geheimdienst GCHQ eh schon sämtliche Kommunikationsdaten abfängt und speichert.

Wer nicht weiß was Vorratsdatenspeicherung eigentlich ist, und warum wir sie ablehnen, dem sei der re:publica Talk von Anna und Andre empfohlen.

0

by Kilian Vieth at July 10, 2014 04:02 PM

Die Geschichte von Hollywood in unter zehn Minuten erklärt:

Die Geschichte von Hollywood in unter zehn Minuten anschaulich erklärt:

0

by Markus Beckedahl at July 10, 2014 02:55 PM

Podcastbus-Prozess: Urteil rechtskräftig, Urteilsbegründung eine wahre Freude

Das Blog Metronaut war 2011 beim Castor-Transport mit seinem Podcast-Equipment, welches samt Bus von der Polizei beschlagnahmt wurde. Metronaut setzte sich vor Gericht dagegen zu wehr und bekam nach drei Jahren Recht. Das Urteil ist jetzt rechtskräftig und die Urteilsbegründung eine wahre Freude für die Blogger. Es ist teilweise absurd, wie das Gericht die Polizei abwatschen muss, weil dort Polizisten "in Urlaubsvertretung" Augenzeugenberichte für Kollegen schreiben. Das hat schon Qualität eines Bananenstaates.

Positiver Nebeneffekt: Das Gericht meinte, es spiele keine Rolle, ob die Metronaut-Blogger im Besitz eines Presseausweis wären (waren sie), den Grundrecht gilt unabhängig von einem Presseausweis:

> "Die Kläger wurden durch die Sicherstellung des VW-Busses nebst der darin befindlichen Gegenstände in ihrem Recht auf freie Rundfunkberichterstattung (Art. 5 Abs. 1 Satz 2, 2. Halbs. GG) verletzt. Der Schutzbereich war unabhängig davon eröffnet, ob die Kläger Inhaber eines Presseausweises waren oder nicht. Presseausweise werden – anders als beispielsweise Rechtsanwaltausweise – nicht von einer öffentlichen Stelle, sondern vom Deutschen Journalistenverband ausgegeben. Voraussetzung für den Erhalt ist die hauptberufliche Tätigkeit als Journalist, die aber gerade nicht Bedingung für einen Schutz durch Art. 5 Abs. 1 GG ist. Der Schutzbereich umfasst nicht nur die Berichterstattung selbst, sondern auch alle wesensmäßig damit zusammenhängenden Tätigkeiten, insbesondere auch die Beschaffung der zu berichtenden Informationen [..]. Durch die streitgegenständliche Sicherstellung wurden die Möglichkeiten der Informationsbeschaffung und -verarbeitung der Kläger erheblich eingeschränkt."

Wir gratulieren zum Erfolg und freuen uns über die gelungene Urteilsbegegründung.

Wir hatten im Vorfeld des Prozesses Hans Gift von Metronaut dazu interviewt: Ist ein Aufnahmegerät eine Gefahr für die Polizei? Verfahren zum Podcast-Bus startet am Donnerstag.

0

by Markus Beckedahl at July 10, 2014 02:18 PM

Militärputsch 2014: Internetsperren in Thailand

Dark Cloud over Democracy in Thailand | Demokratiedenkmal in Thailand von Paul_the_Seeker, flickr | CC-BY-2.0

Das thailändische Militär hat das Land seit dem Putsch am 22. Mai fest im Griff. Um die politische Kontrolle abzusichern und Gegenstimmen zu unterdrücken, greift das Militärregime zu Kommunikationsüberwachung und -zensur, vor allem online. Was wird da gefiltert und blockiert?

Eine Besonderheit dieses Putsches ist, dass das Kriegsrecht bereits zwei Tage vor dem eigentlichen Putsch verhängt wurde. So war es dem Militär möglich, im Vorfeld Rede-, Versammlungs- und Pressefreiheit massiv einzuschränken und so den erfolgreichen Verlauf der Machtübernahme zu gewährleisten. Kurz darauf sorgte die kurzfristige Unzugänglichkeit von Facebook für Schlagzeilen. Citizen Lab, das interdisziplinäre Forschungslabor aus Toronto, hat sich eingehend mit Online-Sperren ab dem Putschzeitpunkt befasst und veröffentlichte gestern einen Bericht über Filterung in Thailand im Zeitraum vom 22. Mai bis 26. Juni.

Die Autoren untersuchen, wie genau in Thailand was online gefiltert wird und welche weiteren Formen der Informationskontrolle im Anschluss an den Putsch angewendet werden. Von 437 getesteten URL waren 56 bei verschiedenen Internetanbietern gesperrt:

> Die Ergebnisse identifizieren insgesamt 56 blockierte URLs im Land. Die blockierten Inhalte beinhalten sowohl politisches Material, wie von inländischen unabhängigen Nachrichtenmedien und internationaler Staatsstreich-kritischer Berichterstatung, als auch Accounts sozialer Medien die Anti-Putsch-Material teilen, sowie Umgehungswerkzeuge, Glücksspielwebseiten und Pornografie.

Dank der kontinuierlichen Testweise konnten die Autoren die dynamische Entwicklung der Filterung feststellen. Je nach sich wandelndem Inhalt und Art der Hoster veränderte sich auch die Art der Sperrung.

Neben den Online-Blockaden führte die Junta noch weitere kommunikationskontrollierende Maßnahmen durch, wie etwa die Schaffung neuer Behörden zur Überwachung und Kontrolle von Online-Inhalten, die Überwachung mobiler Kommunikation, gezieltes Vorgehen gegen Aktivisten und social-network-affine ehemalige Regierungsmitglieder, Befragungen von Akademikern und Journalisten und die Einführung einer App, um Facebook-Anmeldeinformationen abzuschöpfen.

Der Bericht von Citizen Lab ist eher technisch, weist aber auf einen wichtigen Umstand hin: In Zeiten politischer Umbrüche, Krisen und Konflikte ist Kommunikation, vor allem das Internet, ein besonders umkämpftes Gut. Das Militärregime geht mit großer Härte gegen kritische Meinungen vor, setzte Belohnungen für identifizierende Bilder von Demonstranten aus, überwacht Aktivisten und führt Phishingangriffe und Netzsperren durch. Das soll der Stabilisierung der Situation, aber vor allem der Machthaber dienen. Mit einer Demokratie hat das überhaupt nichts zu tun, aber im Kriegsrecht ist alles erlaubt. Dass dabei die eigene Bevölkerung unterdrückt wird,

gerät zur Nebensächlichkeit.

> Whether and to what extent these information controls affect the ICT landscape in Thailand in years to come remains to be seen.

Der längerfristige Einfluss dieser strikten Kontrollmaßnahen muss noch abgewartet werden. Citizen Lab bleibt an der Untersuchung der Lage dran.

0

by Elisabeth Pohl at July 10, 2014 02:17 PM

CDU-Abgeordneter beschwert sich, dass er von ausländischen Diensten überwacht wird

Der Bundestagsabgeordnete Roderich Kiesewetter (CDU), zugleich Obmann der Unionsfraktion im NSA-Untersuchungsausschuss, beschwerte sich jetzt, "dass Dritte auf sein Handy zugegriffen haben. Es sei aber nicht klar, was genau ausländische Dienste abschöpfen." Das berichtet der SWR mit Verweis auf Kiesewetter, der als Bundestagsabgeordneter das Privileg hat, dass sich Techniker der Verwaltung (oder eher vom BSI oder Verfassungsschutz) sein Handy genauer anschauen, während wir Bürger leer ausgehen.

Gleichzeitig fordert er einen besseren Schutz für Abgeordnete vor der Totalüberwachung. Wir fragen uns: Warum nur für Abgeordnete und nicht für alle Bürgerinnen und Bürger?

> Kiesewetter sagte, er habe Anhaltspunkte, dass die Obleute aller vier Parteien im NSA-Untersuchungsausschuss abgehört worden seien.

Die Anhaltspunkte kommen daher, dass das wohl der Verfassungsschutz-Präsident Maaßen vor kurzem den Obleuten der Fraktionen so erklärt hat und dann Kryptohandies verteilte. Auch hier gehen wir als Bürgerinnen und Bürger leider leer aus und müssen zusehen, dass Herr Kiesewetter mal mehr motiviert wird, dabei mitzuhelfen, dass auch unsere Grundrechte durchgesetzt werden können.

Update: Der SWR bezieht sich wohl teilweise auf ein Interview, dass Herr Kiesewetter mit der Schwäbischen Post geführt hat und was hinter einer Paywall versteckt ist. Da findet sich auch noch dieses lustige Zitat:

> Macht es Ihnen nicht Angst, dass es keine Geheimnisse mehr gibt?
>
> Ich habe ein gutes Gewissen und mache mit meinen Bemerkungen (auch am Telefon) den potenziellen Abhörern ein schlechtes. Außerdem bin ich sehr zuversichtlich, dass wir Licht ins Dunkel bringen. Am Ende brauchen wir mehr Datensicherheit für unsere Bürgerinnen und Bürger, unsere Wirtschaft und unsere staatlichen Institutionen. Dafür arbeite ich und das werden wir schaffen.

0

by Markus Beckedahl at July 10, 2014 12:53 PM

New York Times erklärt Netzneutralität: 'A Threat to Internet Freedom'

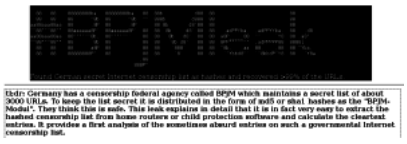
Die New York Times hat auf ihrer Meinungsseite eine kurze Video-Dokumentation zur Debatte um Netzneutralität: 'A Threat to Internet Freedom'.

Gibt es auch als MP4. (66 MB)

0

by Markus Beckedahl at July 10, 2014 12:20 PM

Interview with BPjM-Leaker: Website Blacklists shouldn't be done "in an intransparent way by a government"



Screenshot of the website "BPJM-Leak" with a description of the hack and the extracted list of URLs.

An anonymous hacker has reverse-engineered and published the once-secret blacklist of URLs produced by a German federal agency. He or she did this mainly out of technical curiosity – and found that it was really easy to do. The hacker hopes not go get sued for this action – and offers a general critique on secret, state-sponsored internet censorship.

On Tuesday we reported, that the secret URL blacklist of the German "Federal Department for Media Harmful to Young Persons" was reverse-engineered and published. It contains many dead sites and cases of overblocking, but also "normal porn, animal porn, child/teen porn, violence, suicide, nazi or anorexia." The list is given to internet search engines like Google and DSL/Cable routers, so they can block those URLs.

Yesterday we decided to remove our link to the original website, because the "Commission for the Protection of Minors in the Media" threatened to file a criminal complaint, accusing us of "making child pornography available". Now we have conducted an interview with the anonymous hacker. (*This interview is also available in German, thanks to Kilian for the translation!*)

netzpolitik.org: What was your intention of reverse-engineering the list?

BPjM-Leaker: I did this leak out of (technical) curiosity, basically.

I've stumbled over the md5 hashed BPjM list by chance and was just curious. It was like a "hacker puzzle", I tried to figure out the system how this BPJM-Modul works. Eventually I found the system (md5 hash of URL with http:// in front and no www subdomain, other md5 hash for the path) by manually trying domains I expected to be on the list (rotten.com and youporn.com). Now that the puzzle was solved it involved into a challenge: Try to find each and every domain on this list by collecting huge lists of domains and check if they are on the list. In an ideal world this leak may lead to the end of the BPjM/FSM/KJM/etc. website filtering and the money will be instead spent on pedophile prevention programs…

netzpolitik.org: What is your intention of publishing the list?

BPjM-Leaker: I wasn't sure what would be the best way to deal with this information. Just keep it on my own, send the data to Wikileaks, write an article/blog post with my real name or just leak it on my own with the raw data and technical details how to verify the list? In the end I decided for the last option. By publishing this list everyone can see how ridiculous this list is with its absurd entries.

netzpolitik.org: How much time did the hack take you in total?

BPjM-Leaker: Extracting the list and figuring out the md5 "encryption" system was two evenings if I remember correctly. Collecting all the lists of domains happened over the course of several months, but in total it wasn't that many hours.

netzpolitik.org: Publishing the list is forbidden by German law. Why did you chose to disobey that? Do you expect to get sued? Do you think you will get caught?

BPjM-Leaker: In my opinion it is wrong to collect this list in the first place. Technically the BPjM published the list and I just did a kind of transformation of the data. I hope to stay anonymous. But in fact I didn't do anything special. Anyone with some basic computer knowledge and curiosity should be able to collect this list. Homework in the first semester of studying computer science is usually more difficult. I can't believe nobody did this before and they consider this BPjM-Modul as completely safe for so many years.

netzpolitik.org: We have linked to your site, but the "Commission for the Protection of Minors in the Media" threatened to sue us, because allegedly some of the URLs in the list contain child pornography, illegal after § 184b StGB in Germany.

netzpolitik.org: Do you know of any specific URLs on the list, that host such material? If yes: have you done anything about it?

BPjM-Leaker: Thank you for linking to the website in the first place and thank you for hesitating to remove it and being transparent about it! I am not aware of a domain on the list containing child pornography. At first I tried to do do a deeper analysis of the list entries (like the other analysis by AK-Zensur and Matti Nikki I linked to) by visiting each URL and categorize them manually. But 3000 stupid websites was just too much to visit and I gave up pretty quickly.

netzpolitik.org: Would you be willing to take down URLs on your list, when provided with URLs that contain such material?

BPjM-Leaker: If I am aware of URLs on the list which contain such material I would write a mail to the abuse contact of both the domain registrar and the hoster. Reporting the URL to local authorities of the country the website is hosted in would also be a good idea. Then I would expect the website to be taken down in a matter of hours. If I know a domain contains child abuse material I would replace the URL with its md5 hash.

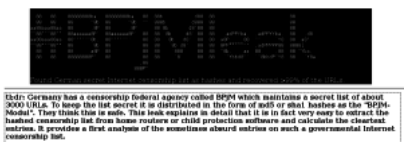
netzpolitik.org: What's your general opinion on blacklists like that? Should states produce blacklists for child/youth protection? Should they be mandatory? Should they be secret?

BPjM-Leaker: For me it feels wrong that there are many different laws for different people. Depending on the country you live in and your age other people decide what you are allowed to see. In China they have their huge censorship infrastructure, in the UK they block file sharing, in Germany they block websites selling old helmets because they have a swastika on them. If the list is secret there is no control and as a result the quality of the entries is really bad as this BPjM example proves. Filtering websites for child protection might be a useful tool in some cases but not in an intransparent way by a government.

0

by Andre Meister at July 10, 2014 10:57 AM

BPjM-Leaker im Interview: "Erfahre ich von Kinderpornografie, nehme ich das von der Liste und aus dem Netz"



Screenshot der Seite mit Beschreibung des Hacks und veröffentlichter Liste.

Falls es auf der veröffentlichten Liste indizierter Webseiten wirklich Kinderpornografie geben sollte, würde der Leaker diese URLs entfernen und sich für die Löschung der Inhalte einsetzen. Das sagte der oder die anonyme Hackerin im Interview mit netzpolitik.org. Eigentlich war sie nur neugierig und wollte die technische Herausforderung lösen – das war einfacher als eine Uni-Hausaufgabe. Er äußert Verständnis für unsere Entscheidung, den Link zu entfernen – und grundsätzliche Kritik an geheimen Sperrlisten.

Am Dienstag haben wir darüber berichtet, dass die geheime Liste in Deutschland indizierter Webseiten veröffentlicht wurde. Gestern haben wir uns entschieden, den Link zur Originalseite herauszunehmen, da die KJM gedroht hat, uns wegen "Zugänglichmachung von Kinderpornografie" anzuzeigen. Jetzt haben wir ein Interview mit dem oder der anonymen Hacker/in geführt. (*Hier gibt's das auch auf englisch, danke an Kilian für's Übersetzen!*)

netzpolitik.org: Warum hast du die Liste reverse-engineered?

BPjM-Leaker: Ich habe das im Grunde aus (technischer) Neugier gemacht.

Ich bin zufällig über die MD5-gehashte BPjM-Liste gestolpert und war einfach neugierig. Es war wie ein "Hacker-Puzzle", ich habe versucht, herauszufinden, wie das BPjM-Modul funktioniert. Schließlich habe ich das System herausgefunden (MD5-Hash-URL mit http:// am Anfang und ohne www-Subdomain, anderer MD5-Hash für den Pfad) und probierte manuell Domains aus, die ich auf der Liste vermutete (rotten.com und youporn.com). Jetzt, da das Rätsel gelöst war, entwickelte es sich zu einer neuen Herausforderung: ich versuchte alle Domains auf dieser Liste zu finden, indem ich riesige Listen von Domains sammelte und dann abglich, ob sie auch auf der BPjM-Liste sind. In einer idealen Welt würde dieser Leak zum Ende der Netz-Filter von der BPjM/FSM/KJM führen und das Geld würde stattdessen für Pädophilen-Präventionsprogramme ausgegeben…

netzpolitik.org: Warum hast du die Liste veröffentlicht?

BPjM-Leaker: Ich war mir nicht sicher, was der beste Weg ist, mit diesen Informationen umzugehen. Sie einfach für mich behalten, die Daten an WikiLeaks schicken, einen Artikel/Blog-Post mit meinen echten Namen schreiben, oder sie einfach selbst leaken, mit den Rohdaten und den technischen Details wie die Liste zu überprüfen ist? Am Ende habe ich mich für die letzte Option entschieden. Durch die Veröffentlichung der Liste können jetzt alle sehen, wie lächerlich sie ist, mit ihren absurden Einträgen.

netzpolitik.org: Wie viel Zeit hast du für den Hack insgesamt gebraucht?

BPjM-Leaker: Die Liste zu extrahieren und das MD5-"Verschlüsselungs"-System herauszufinden waren zwei Abende, wenn ich mich richtig erinnere. Die ganzen Domain-Listen sammelte ich über mehrere Monaten, aber insgesamt waren es nicht so viele Stunden.

netzpolitik.org: Die Veröffentlichung der Liste ist nach deutschem Recht verboten. Warum hast du dich entschlossen, es trotzdem zu tun? Erwartest du, angezeigt zu werden? Glaubst du, dass du erwischt wirst?

BPjM-Leaker: Meiner Meinung nach ist es falsch, diese Liste überhaupt anzulegen. Technisch gesehen hat die BPjM die Liste veröffentlicht und ich habe nur eine Art von Transformation der Daten vorgenommen. Ich hoffe, anonym zu bleiben. Eigentlich habe ich nichts Besonderes getan. Alle, die grundlegende Computer-Kenntnisse haben und und neugierig sind, dürften in der Lage sein, an diese Liste zu gelangen. Die Hausaufgaben im ersten Semester eines Informatikstudiums sind in der Regel schwieriger. Ich kann nicht glauben, dass das bisher niemand gemacht hat und dieses BPjM-Modul jahrelang als völlig sicher angesehen wurde.

netzpolitik.org: Wir hatten deine Website verlinkt, aber die KJM hat gedroht, uns zu verklagen, weil angeblich einige der URLs in der Liste Kinderpornografie enthalten, was in Deutschland nach § 184b StGB illegal ist. Kennst du irgendwelche konkreten URLs auf der Liste, die solches Material hosten? Wenn ja: Hast du etwas dagegen getan?

BPjM-Leaker: Erst einmal vielen Dank für das Verlinken auf die Webseite! Und danke auch, dass ihr gezögert habt, den Link wieder zu entfernen und transparent darüber berichtet! Ich kenne keine Domain auf der Liste, die Kinderpornografie beinhaltet. Zuerst habe ich versuchte, die Listeneinträge genauer zu analysieren, indem ich jede URL einzeln aufrief und dann manuell kategorisierte (wie die anderen Analysen des AK-Zensur und von Matti Nikki, die ich verlinkt habe). Aber 3.000 blöde Webseiten anzugucken war mir einfach zu viel und ich habe ziemlich schnell aufgegeben.

netzpolitik.org: Wärst du bereit, URLs von der Liste zu nehmen, wenn dir konkret welche genannt werden, die solches Material enthalten?

BPjM-Leaker: Wenn ich von URLs auf der Liste erfahren würde, die solches Material enthalten, würde ich sowohl eine Abuse-Mail an sowohl den Domain-Kontakt als auch den Hoster schreiben und den Missbrauch melden. Die zuständigen Behörden des Landes, in dem die Website gehostet wird, über die URL zu informieren, wäre auch eine gute Idee. Dann würde ich erwarten, dass die Website innerhalb weniger Stunden vom Netz genommen wird. Wenn ich weiß, dass eine Domain Material über Kindesmissbrauch enthält, würde ich die URL mit ihrem MD5-Hash ersetzen.

netzpolitik.org: Was ist deine Meinung zu Blacklists im Allgemeinen? Sollte Staaten Blacklists für Kinder-/Jugendschutz erstellen? Sollten die verpflichtend sein? Sollten sie geheim sein?

BPjM-Leaker: Für mich fühlt es sich falsch an, dass es viele unterschiedliche Gesetze für verschiedene Menschen gibt. Je nachdem, in welchem Land du lebst und wie alt du bist, entscheiden andere Menschen, was du sehen darfst. In China haben sie ihre große Zensur-Infrastruktur, in Großbritannien wird Filesharing gesperrt, in Deutschland werden Webseiten gesperrt, die alte Helme verkaufen, weil da ein Hakenkreuz drauf ist. Wenn die Liste geheim ist, gibt es keine Kontrolle und dadurch ist die Qualität der Einträge wirklich schlecht, wie das aktuelle BPjM-Beispiel beweist. Die Filterung von Webseiten zum Kinderschutz könnte in einigen Fällen ein nützliches Werkzeug sein, aber nicht durch eine Regierung und nicht auf eine intransparente Art und Weise.

netzpolitik.org: Vielen Dank für das Interview.

(***Anmerkung**: Gender-Rants in den Kommentaren könnt ihr euch sparen. Ich werde keine "Ratschläge" annehmen. Meint wer, sich trotzdem aufregen zu müssen, gibt's hatr. Danke für das Verständnis.*)

0

by Andre Meister at July 10, 2014 10:57 AM

Das Experiment

Hier veröffentlichen wir einen Gastbeitrag von Friedemann Karig über das sogenannte "Facebook-Experiment" und seine Konsequenzen. Wir hatten auch schon hier darüber berichtet.

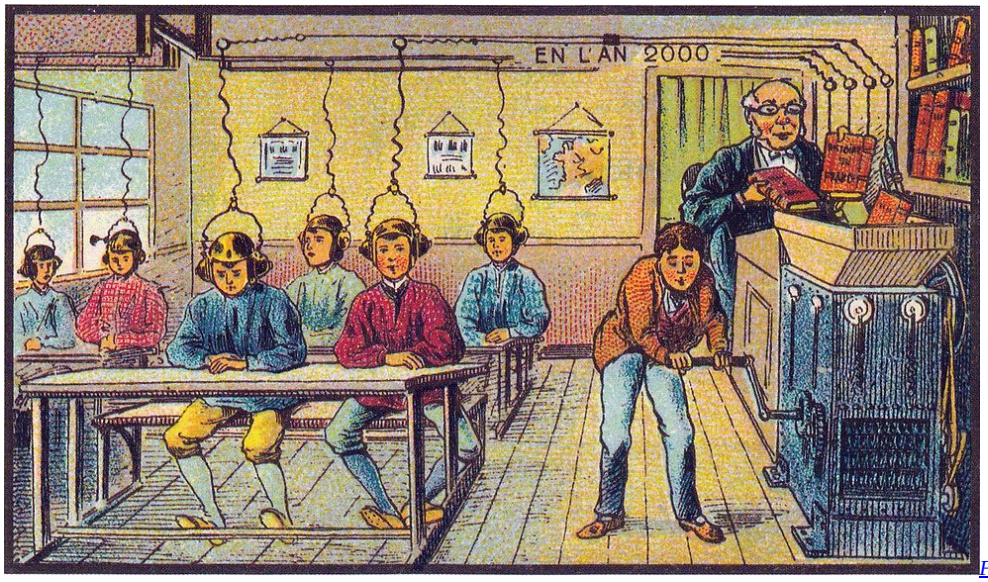
Die schlechte Nachricht: Facebook hat 689003 User für einen Menschenversuch missbraucht.

Im Zuge einer kürzlich veröffentlichten Studie mit dem schönen Namen *"Experimental evidence of massive-scale emotional contagion through social Networks"*, die Facebook 2012 gemeinsam mit der Cornell University durchführte.

Die Forschungsfrage: Was passiert, wenn man das Ausmaß von positiven bzw. negativen Äußerungen in den Timelines und Newsfeeds der User erhöht?

Das Ergebnis: Wer mehr positives liest, postet mehr positives. Wer mehr negatives liest, postet negativer. Die ahnungslosen Probanden äußerten sich im Schnitt um 3% besser oder schlechter gelaunt. Damit ist bewiesen: Gefühle sind ansteckend. Auch im digitalen Raum. Und: die User äußerten sich rein quantitativ *mehr*, je mehr gefühliges sie gelesen hatten. Was für ein soziales Netzwerk eine wichtige Information ist. Facebook manipulierte also die Gefühle seiner Nutzer um zu lernen, wie und warum diese aktiver werden.

Die gute Nachricht: Facebook macht *genau das* jeden Tag. Mit uns allen. Sie veröffentlichen es nur nicht. Aber ist das wirklich eine gute Nachricht? Und dürfen die das überhaupt?



Facebook im Jahr 1907

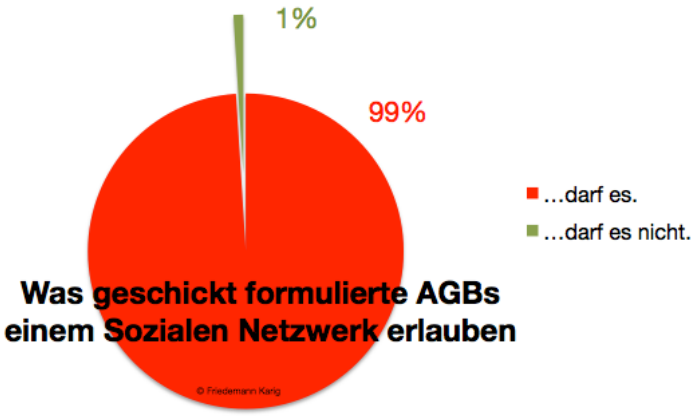
Dürfen die das?

Facebooks Algorithmus – formerly known as "EdgeRank" (oder wie auch immer sie ihn momentan nennen) – bestimmt, was in welcher Gewichtung in den Newsfeed und die Timeline eingespeist wird und was nicht. Er wird fortlaufend optimiert. Dazu schauen die Nerds bei Facebook, wie in jeder Forschungs- und Entwicklungsabteilung, ziemlich genau hin, *wie* User auf *welche* Veränderung reagieren.
Man will wissen, was sie annehmen und was nicht, beispielsweise welche Werbung unter welchen Umständen am besten "klickt". Und das findet man nur heraus, indem man Thesen aufstellt und sie falsifiziert, am lebenden Objekt.

Eigentlich macht das jede Webseite und jeder Online-Händler. Sie nennen es "A/B-Testing": Welche Alternative gefällt den Usern besser im Sinne von "wird mehr geklickt"? Ah, okay, die mit rosa, dann nehmen wir die. Achtung, stark vereinfachender Vergleich: Jeder Bäcker testet A/B, wenn er die Marmeladenfüllung seiner Croissants variiert und seine Kunden nach dem Verputzen der Hörnchen befragt, welches am besten geschmeckt hat.

Die jetzt veröffentlichte Forschung hat technisch also nichts anderes getan, als Facebook und jeder andere (fleißige) Dienstleister macht, sogar machen muss, um sein Angebot zu optimieren. *"Every ad based company exists to alter how you perceive the world"* schreibt Andrew Ledvina, ein ehemaliger "Data Scientist" bei Facebook.
Deswegen hat auch das hinzugezogene Institutional Review Board (IRB), das in den USA jede Forschung am Menschen absegnen muss, das Experiment zugelassen: Facebook führt vergleichbare Untersuchungen sowieso ständig durch, argumentierten die beteiligten Forscher.

Aber darf Facebook seine User der Wissenschaft überlassen?
Dieses spezielle Experiment, anders als Facebook-interne Forschung, hat ein wissenschaftliches Erkenntnisinteresse formuliert und entsprechende Ergebnisse veröffentlicht. Es hat nicht primär im Sinne des Produktes geforscht (das auch nicht immer unbedingt im Sinne des Nutzers sein muss), sondern im Sinne einer Forschungsfrage.
Die Nutzung der User(-Daten) zu Forschungszwecken war angeblich von den Facebook-AGBs abgedeckt. Als User erklärt man sich bereit, dass Daten und Profile für *"for internal operations, including troubleshooting, data analysis, testing, research and service improvement"* genutzt werden. Dass die AGBs "niemand" im Sinne von "fast niemand" liest, ist unser Problem, nicht das von Facebook. Dass der Zusatz *"research"* erst *nach* der Studie in die AGBs kam, schon. Facebook wird dennoch argumentieren, auch dieses Experiment diene letztlich der Verbesserung des Service (*"service improvement"*), weswegen es legal im Sinne der AGBs sei.
Für die Zukunft spielt das keine Rolle, denn jeder Anbieter wird einfach wie Facebook das unverfängliche Wort *"research"* in seine AGBs aufnehmen, um sich abzusichern. Daraus ergibt sich folgende Grafik:



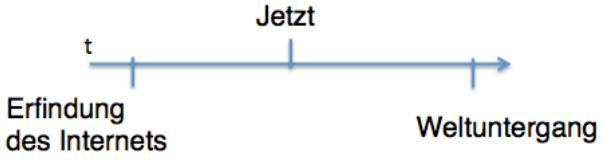
Hölle, Hölle, Hölle!

Kritisch an dieser eigentlich nur logischen Nutzung des Datenschatzes bleibt jedoch die "Manipulation" von Emotionen. Wie schon Wolle Petry klagte: *"Das ist Wahnsinn. Du spielst mit meinen Gefühlen."* Was wäre, wenn jemand der (negativ) manipulierten Personen sich oder anderen etwas angetan hätte? Hölle Hölle Hölle?
Wir introvertierten Emotionsverweigerer wissen: Gefühle *empfinden* und Gefühle *ausdrücken* ist nicht das gleiche. Und die Studie zielte auf einen minimalen Einfluss ab: *"…the result was that people produced an average of one fewer emotional word, per thousand words."* Eine Veränderung des emotionalen Ausdrucks im Promillebereich kann schwer als massive Manipulation von Gefühlen gelten. Und auch wenn das forschende Fingern an sogenannten "Sentimenten", also Gefühlszuständen, auf den ersten Blick anrüchig erscheint (und auf den zweiten Blick auch wissenschaftlich mindervalide, aber das ist eine andere Geschichte): Ein Kaufreflex ist ebenso eine Gefühlsregung, ein Verlangen, das die Werbung gezielt reizt. Wo genau verläuft die Grenze zwischen Manipulation zu Abverkaufszwecken, die oft nicht nur positive Gefühle anspricht, sondern Menschen auch gezielt ein schlechtes Gewissen macht, und der Manipulation zu Gunsten einer kommunikativen Aktivierung?

Im wissenschaftsethischen Sinne wiegt schwerer, dass die Teilnehmer nicht über die Studie informiert wurden, es also keinen *"informed consent"* gab, wie er bei Versuchen mit Menschen vorgeschrieben ist. Eine ethische Wissenschaft informiert freiwillige Probanden oder versucht, falls das Studiendesign die Unwissenheit der Probanden vorschreibt, sich über Dritte abzusichern und sie direkt nach dem Versuch zu informieren.
Und auch wenn Facebook ein von seinen AGBs geschütztes Unternehmen ist, gelten vom moralischen Standpunkt her die Regeln vergleichbarer wissenschaftlicher Unternehmungen. Zumindest für die Forscher. Sie hätten darauf bestehen müssen, dass keine Probanden ohne echte informierte Zustimmung Teil des Experimentes werden. Bis jetzt schweigen die Teile der Scientific Community jedoch, die betroffen sind. Wahrscheinlich, weil der Honigtopf der Big Data sie alle lockt. In Zukunft müssen sie sich die Frage stellen, welche Art von Big-Data-Forschung wissenschaftsethisch vertretbar ist.

Im Sinne unternehmerischer Fairness hätte Facebook eine einfache Abfrage vorschalten müssen, ob die User einverstanden sind, an solch einer Studie teilzunehmen. Es fänden sich sicher 700000, die sich der Forschung nicht nur durch AGBs legalisiert, sondern durch einen "informed consent" legitimiert zur Verfügung stellen. Und die Ergebnisse dieser Forschung müssten transparent allen zur Verfügung stehen. Was in diesem Fall passierte und paradoxerweise erst zur Empörung führte.

Aber warum fühlt sich das alles nicht nur falsch, sondern bedrohlich und böse an? Warum erledigt sich das Problem nicht, wenn Facebook das nächste Mal vorher nachfragt? Was passiert als nächstes?



Der Kunde als Experiment

Subjektiv fühlt sich natürlich der Eingriff in die eigene "Privatsphäre" mies an. Meine Timeline, mein Newsfeed, mein Profil sind für mich *privat*. In diesem digitalen Abbild meines Soziotopes will ich der Souverän sein. Und normalerweise empfinde ich mich auch als solchen. Auch, weil Facebook mir suggeriert, ich könne per Einstellungen und Abos und Freundschaften und "Verbergen" weitgehend über "mein" Facebook bestimmen.
Was nicht richtig ist. Facebook bestimmt.
Es ist ihr Produkt.

So wie ein mit Marmelade gefülltes Croissant das Produkt eines Bäckers ist. Ich kann darauf verzichten, wenn es mir nicht schmeckt. Aber ich kann es nicht endgültig beeinflussen. Das letzte Wort hat immer der Anbieter. Und die Anbieter suchen emsig nach Möglichkeiten, den Datenschatz zu heben. Sie werden nicht aufhören, die Daten für alles zu gebrauchen, was man zulässt. Und offensichtlich schrecken sie dabei vor nichts zurück.
Langfristig an Gefühlen rumspielen ist etwas anderes als einen kurzfristigen Kaufreflex zu triggern. 700000 User schlechter gelaunt machen ist etwas anderes, als ihnen Viagra anzudrehen.

Und das ist genau die Lektion, die wir aus diesem ersten öffentlichen Fall eines Big-Data-Missbrauchs lernen sollten: Wir können keine

digitale Fairness von profitorientierten Unternehmen erwarten. Inzwischen ist es eine alte digitale Weisheit:
Wenn etwas umsonst ist, bin ich nicht der Kunde. Sondern das Produkt.
Oder das Experiment.

Facebook im Jahr 1964

Heimliche Verführer

Das Facebook-Experiment lässt die Möglichkeiten dieser Unternehmen, aber auch der Politik und anderer Institutionen, die sich ihrer bedienen, erahnen. Sie machen mir Angst. Und erinnern Sebastian Deterding an eine Schöne Neue Welt: *"Manipulations like these show how much power online companies like Facebook have over us, and filtering information by sentiment could keep us in a Huxleyan SNAFU bubble."*

Dieses "Social Engineering" auf Basis von Big Data macht uns alle zu Versuchskanninchen, um in unsere Köpfe zu schauen und unser Verhalten zu beeinflussen. Ja, das macht die Werbung seit Jahrzehnten. Aber sie hatte niemals die Macht der Big Data. Sie arbeitete mit groben Clustern, Sinus-Milieus, Zielgruppen. Nicht auf der Ebene der Individuen.
Und sie hatte niemals diese Effizienz: Die Studie wurde von drei Personen durchgeführt, *"one member of Facebook's own Core Data Science team and two university researchers from Cornell and UCSF"*. Drei Menschen konnten 700000 andere Menschen studieren. Und das um einiges genauer, als es früher möglich war: *"If the 20th century engineers of consent had magnifying glasses and baseball bats, those of the 21st century have acquired telescopes, microscopes and scalpels in the shape of algorithms and analytics,"* vergleicht Zeynep Tufekci.

Genau jetzt, angesichts solcher Beispiele, ist die Zeit sich dagegen zu wehren, dass Akteure wie Facebook ihre Macht ausnutzen. Tufekci warnt: *"…these large corporations (and governments and political campaigns) now have new tools and stealth methods to quietly model our personality, our vulnerabilities, identify our networks, and effectively nudge and shape our ideas, desires and dreams."*

Facebook im Jahr 2024 (und im schwedischen Animationsfilm Metropia, von dessen Filmplakat der Ausschnitt stammt)

Facebook als Fernbedienung

Das ist das Problem an solchen Experimenten und an den Systemen, die sie erst ermöglichen: Nicht, dass sie illegal, fantasie- und absichtsvoll böse wären. Das sind sie nicht automatisch, auch wenn sie sich so anfühlen mögen.
Sondern, dass sie eben nur ein ganz kleiner Schritt von alltäglichen, legitimen Praktiken entfernt sind. Dass sie ein bisschen wie normale Werbung aussehen. Dass sie aufsetzen auf einer längst akzeptierten Realitätskonstruktion durch intransparente Anbieter. Dass sie auf Grund der Größenordnung und Heimlichkeit einerseits so effizient und andererseits so leicht zu verbergen sind. Dass sie unseren Kontrollverlust nicht erfinden, sondern nur ausnutzen.

Dieses *"Social Engineering"* ist gefährlich, obwohl oder gerade weil es per se nichts neues oder böses ist. Sondern weil es letztlich unsichtbare Kontrolle ermöglicht. Willensbildung wird weniger öffentlich, weniger bewusst, weniger selbstständig. Big Data, richtig (oder eher falsch) genutzt, wird zur Fernbedienung für unsere Köpfe.

Nichts im Netz ist objektiv oder neutral. Umso genauer müssen wir hinschauen, wer uns etwas warum für objektiv oder neutral verkaufen will. Und noch wichtiger: Nichts ist umsonst. Umso klarer müssen wir sehen, was es kostet.

tl;dr: Big Data kann missbraucht werden, wehret den Anfängen.

0

by Gastbeitrag at July 10, 2014 10:36 AM

Mit einem Luftschiff über die NSA fliegen und Luftaufnahmen machen

Die EFF ist zuletzt zusammen mit Greenpeace USA mit einem ~~Zeppelin~~ Blimp über das neue Daten-Center der NSA in Utah geflogen und hat den Protestflug auch für Luftaufnahmen genutzt.

Davon gibt es auch ein Video:

Jetzt gibt es High-Res Aufnahmen von oben: Releasing a Public Domain Image of the NSA's Utah Data Center.

0

by Markus Beckedahl at July 10, 2014 09:24 AM

Ausschuss-Posse um Zeugenvernehmung: Edward Snowden kann in Berlin viel mehr aussagen als in Moskau

Guter Grund, die Regierung zu verklagen: Edward Snowden.

Edward Snowden steht dem NSA-Untersuchungsausschuss weiterhin als Zeuge zur Verfügung. Offen reden kann er jedoch in Moskau nicht, weder bei Tee – noch per Video. Das geht aus einem Brief seines deutschen Anwalts hervor, den wir veröffentlichen. Die Opposition will auf seine Vernehmung in Deutschland klagen.

Im Untersuchungsausschuss zur Geheimdienstüberwachung ("NSA-Ausschuss") spielt sich ein unwürdiges Theater um die Anhörung von Edward Snowden ab. Obwohl der Ausschuss einstimmig beschlossen hat, die Person, ohne die es den Ausschuss gar nicht gäbe, als Zeuge zu vernehmen, saugen sich die Regierungsparteien einen Grund nach dem nächsten aus den Fingern, um den Whistleblower ja nicht nach Deutschland holen zu müssen. Die Ausreden werden so absurd, dass man sich teilweise fragt, warum sie dem überhaupt erst zugestimmt haben, wenn sie doch anscheinend um jeden Preis die befürchtete Kritik der USA an einer Anhörung Snowdens in Deutschland verhindern wollen.

Am 20. Juni haben wir berichtet, dass Snowden dem Ausschuss ausführliche Aussagen "zu konkreten Tatsachen und Ereignissen" anbietet – jedoch nicht in Moskau, weil seine Situation das dort nicht erlaubt. In der medialen Öffentlichkeit wurde dieses Detail meist unterschlagen und oft unzureichend verkürzt: "Snowden lehnt Befragung in Moskau ab".

Und jetzt erneut: "Snowden sagt Video-Vernehmung ab". Das ist aber wieder nur verkürzt. Wir haben erneut den vollständigen Brief erhalten, den Snowdens deutscher Anwalt Wolfgang Kaleck an den Ausschuss geschickt hat und veröffentlichen den an dieser Stelle. Der lautet in Volltext:

> Sehr geehrter Herr Prof. Dr Patrick Sensburg,
> sehr geehrte Damen und Herren Obleute,
>
> vielen Dank für die Übersendung der Beschlüsse des Ausschusses vom 26. Juni 2014.
>
> Aus den bereits mehrfach dargelegten Gründen, insbesondere wegen der damit verbundenen Sicherheitsrisiken, steht der Zeuge Edward Snowden – trotz grundsätzlicher Aussagebereitschaft – für die avisierte Videovernehmung in Moskau nicht zur Verfügung.

> Im Grunde möchte ich mich jedes Kommentares über die diversen öffentlichen Äußerungen von Ausschussmitgliedern enthalten. Aufgrund der Beharrlichkeit mit der seine Zeugenaussage vor dem Parlamentarischen Untersuchungssauschuss mit seinen Auftritten in anderen Foren verglichen wird, empfehle ich rein vorsorglich eine Inaugenscheinnahme des Videos seiner Expertenstellungnahme vor der Parlamentarischen Versammlung des Europarates am 24. Juni 2014, in der **Herr Snowden während seiner anschließenden kurzen Befragung klarstellt, dass er ausschließlich als Experte und nicht als Zeuge zur Verfügung stand und daher auch die Beantwortung von Fragen zu konkreten Sachverhalten ablehnt**.
>
> Mit freundlichen Grüßen
>
> Kaleck, Rechtsanwalt

Snowden kann in Deutschland vor dem Ausschuss als Zeuge viel mehr aussagen als in Moskau oder anderswo. Das ist der Deal für sein vorläufiges Asyl in Russland. Hinter vorgehaltener Hand sehen das auch die schwarz-roten Abgeordneten ein. Sie wollen ihm nur kein freies Geleit geben müssen. Diese Position vertrat gestern auch der ehemalige Geheimdienstkoordinator der Bundesregierung Bernd Schmidbauer in einer Diskussion. Wenig später ließ er dann einen weiteren Grund durchscheinen: Für ihn sind Whistleblower, die Geheimnisse ihrer Dienste öffentlich machen, Verräter. Kein Wunder, dass man ihn da lieber in ~~Guantanamo~~Fort Meade sieht als in Berlin.

Immerhin nimmt die Opposition ihre Rolle als Aufklärer ernst und kündigt Klage gegen die Bundesregierung an, wenn diese eine Zeugenanhörung in Deutschland weiter blockiert. Das haben die drei Sachverständigen Juristen dem Ausschuss in seiner ersten öffentlichen Sitzung ja auch wiederholt geraten. Also: Regierung verklagen!

0

by Andre Meister at July 10, 2014 09:21 AM

Schäuble: Kanzlerin not amused, dass die USA drittklassige Spione bei uns haben

Dabei müssten die USA doch nur direkt oben anfragen und bekämen alle Infos oder wie muss man das verstehen?

> Mit der Anwerbung von deutschen Spionen schürten die USA Gefühle wie Misstrauen und Distanz in Deutschland, sagte Schäuble. “Das ist ja sowas von blöd.” Zwar hätte Deutschland ohne die Partnerschaft mit US-Geheimdiensten viele Terrorbedrohungen nicht abwehren können, dies heiße aber nicht, “dass die Amerikaner drittklassige Leute bei uns anwerben dürfen”. “Über so viel Dummheit kann man auch nur weinen. Deswegen ist die Kanzlerin da auch ‘not amused’.” Gleichwohl fühle er sich von den “Amerikanern weniger bedroht als von manchen anderen in der Welt”. Man solle “die Kirche zwischendurch auch mal im Dorf lassen”.

0

by Markus Beckedahl at July 10, 2014 06:42 AM

CCC Dresden

Grillen am Freitag

Datum
Freitag, 11. Juli 2014 um 20:30 Uhr
Ort
GCHQ, Lingnerallee 3

Nicht vergessen: am Freitag findet der Themenabend Open Source und Faire IT statt.

Hinterher wird mit Partylaune gegrillt. (Vorbereitungspad)

by CCC Dresden (mail@c3d2.de) at July 10, 2014 01:00 AM

July 09, 2014

Netzpolitik.org

SPD, IG Metall und Airbus-Betriebsrat werben für “europäische Drohne”

Der “Talarion” von EADS (Modell) war der erste Versuch, eine “europäische Drohne” auf

den Weg zu bringen.

Gab es einmal eine Zeit, in der sich Gewerkschaften und Betriebsräte kritisch gegenüber Rüstungprojekten gezeigt haben? Die ist dann jedenfalls vorbei.

Die Bundesregierung will bekanntlich Drohnen der sogenannten “MALE”-Klasse beschaffen. Diese hochfliegenden Flugroboter könnten zu Aufklärungszwecken und Kampfeinsätzen unterschiedlich eingerüstet werden. Mehrfach hatte EADS (jetzt umbenannt in Airbus Defence and Space) versucht, die Bundesregierung zur Entwicklung einer “europäischen Drohne” zu überreden. Auch die SPD hat sich letztes Jahr dazu bekannt.

Der Betriebsratsvorsitzende von Airbus Defence and Space, Thomas Pretzl, hat sich im Bayerischen Rundfunk zum Thema zu Wort gemeldet. Ihn besorgt die Unsicherheit, ob die “Entwicklung und die Wartung für die neuen Drohnen” nach Manching kommt oder womöglich in anderen Ländern gefertigt wird.

Die IG Metall hatte sich am Wochenende ähnlich geäußert. Die “Welt am Sonntag” interviewte den für Airbus im bayerischen Manching zuständigen Beauftragten, Bernhard Stiedl. Weil Airbus bis 2017 alle bestellten Eurofighter-Kampfjets produziert hat, sorgt man sich nun um die Arbeit der Betriebsangehörigen. Stiedl meint, ein “Drohnenprogramm” könne “zu neuer Beschäftigung führen” und sei deshalb ein “Lichtblick”:

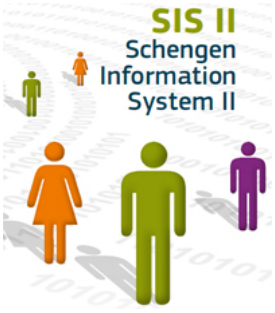
> Ein europäisches Drohnenprogramm würde am Standort Manching 1500 Arbeitsplätze sichern. [...] Wir fühlen uns von der Politik im Stich gelassen. [...] In der Krise gab es Hilfsprogramme für die Auto- und Bankenindustrie. Wir stellen fest, dass das für die Wehrindustrie nicht gilt.

Endgültig entschieden ist übrigens nichts: Zwar tat die Verteidigungsministerin in der “BILD” ihre Überzeugung kund, “in die Entwicklung einer europäischen bewaffnungsfähigen Drohne einsteigen [zu] müssen”. Mit welchen Regierungen, soll nun sondiert werden – denn die sollen die spätere Abnahme in bestimmter Stückzahl garantieren. Ein entsprechendes Angebot hatten zuletzt Airbus und die französische Dassault Aviation sowie die italienische Alenia gemacht.

0

by Matthias Monroy at July 09, 2014 05:52 PM

Polizeilicher Datentausch wird unübersichtlich – EU schlägt “einzige Anlaufstelle” in allen 28 Mitgliedstaaten vor



Das Schengener Informationssystem ist nur eine von ganz vielen Möglichkeiten des polizeilichen Austauschs in der EU. Es wird langsam kompliziert.

Viel zu viele Daten, viel zu unübersichtliche Zuständigkeiten: Sogar Sicherheitsbehörden kommen angesichts der Anzahl polizeilicher Datensammlungen durcheinander. Um die alten und neuen Datenbanken zukünftig einheitlich zu führen, hat die Europäische Union in Estland und Frankreich eine Agentur für das “Betriebsmanagement von IT-Großsystemen” eingerichtet. Derzeit werden dort das Visa-Informationssystem, die Finderabdruckdatenbank und das Schengener Informationssystem verwaltet. Bald könnte die vom deutschen Bundesinnenministerium beworbene Vorratsdatenspeicherung aller Ein- und Ausreisen in die EU hinzukommen.

Allerdings gibt es weit mehr als diese drei Plattformen: Daten werden über die EU-Agentur Europol oder die internationale Polizeiorganisation Interpol weitergegeben, Grenzbehörden nutzen ein Zollinformationssystem. Geregelt werden müssen die Entgegennahme des europäischen oder internationalen Haftbefehls oder von Rechtshilfeersuchen für Hausdurchsuchungen oder Abhörmaßnahmen. Weitere Kanäle der digitalen Zusammenarbeit sind die über 40 Zentren für die Polizei- und Zollzusammenarbeit, die bei verschiedenen Behörden angesiedelten “Verbindungsbeamten” oder Koordinierungsstellen für die Betrugsbekämpfung. Im “schwedischen Rahmenbeschluss” und dem “Vertrag von Prüm” sind ebenfalls Absprachen zum Datentausch festgelegt. Getauscht werden DNA-Profile, Fingerabdrücke und Daten aus Fahrzeugregistern.

Entsprechende Ersuchen zur Weitergabe digitaler Informationen müssen in manchen Ländern bei unterschiedlichen Stellen eingereicht werden. So ist manchmal ein Innenministerium, eine Zollbehörde oder auch einzelne Polizeistellen für die einzelnen Datensammlungen verantwortlich. Diese Zuständigkeiten sind in eigens dafür geschriebenen Handbüchern niedergelegt.

“Single Point of Contact”

Zukünftig soll der Informationsaustausch aber noch einfacher werden. In einem Ratsdokument wird nun die Einrichtung einer einzigen Anlaufstelle für alle Behörden vorgeschlagen. In jedem der 28 EU-Mitgliedstaaten soll dann ein “Single Point of Contact” für den internationalen “Austausch von strafverfolgungsrelavanten Informationen” zuständig sein. Die Plattformen werden der Verantwortung eines federführenden Ministeriums unterstellt. Gewöhnlich ist dies ein Innenministerium. Die eigentliche Arbeit soll aber eine “federführende Stelle” übernehmen. Normalerweise wird dies von einer Kriminalpolizei verrichtet.

Jeder “Single Point of Contact” ist eine Anlaufstelle mit weitreichenden Kompetenzen. Sie wäre an das EU-Intranet sowie das interne Kommunikationssystem von Europol angeschlossen und dürfte darüber Verschlusssachen austauschen. Über Interpol würden alle Ausschreibungen an den “Single Point of Contact” gerichtet. Die Anlaufstelle wäre auch zuständig für offene und verdeckte Fahndungen über das Schengener Informationssystem. Im Falle Deutschlands sind derartige Kompetenzen bereits beim Bundeskriminalamt in Wiesbaden zentralisiert. Dort werden auch Anfragen aus den Bundesländern verwaltet.

Eines der Probleme im unübersichtlichen Informationsaustausch ist das mehrfache Stellen von Ersuchen über mehrere Kanäle. Damit soll nun Schluss sein, wenn alle Ersuchen nur noch über den “Single Point of Contact” laufen. Dieser einzige “Übermittlungskanal” darf während eines laufenden Vorgangs nicht mehr gewechselt werden.

Der “Single Point of Contact” soll aber auch über einen Vollzugriff auf nationale, polizeiliche Datenbanken verfügen. Hierfür sollen die Anlaufstellen an das Intranet ihrer jeweiligen Regierungen bzw. Sicherheitsbehörden angeschlossen werden. Für Telefon, Fax und E-Mail werden Reserve-Kommunikationsverbindungen vorgehalten. Die Anlaufstellen erhalten eigene, moderne elektronische Fallverwaltungssysteme.

Anbindung von “Telefon- und sonstigen Telekommunikationsunternehmen”

Doch damit nicht genug: Die neuen Anlaufstellen sollen über “Zugang zum größtmöglichen Spektrum an einschlägigen nationalen Datenbanken” verfügen. In dem Ratsdokument heißt es dazu:

> Dies erstreckt sich insbesondere auf Datenbanken auf dem Gebiet der Strafverfolgung, Datenbanken für Identitätsdokumente, Fahrzeugregister, nationale Visadatenbanken, Datenbanken der Ausländerbehörden, Häftlingsdatenbanken, DNA-Datenbanken, Fingerabdruckdatenbanken, den Informationsaustausch mit den nationalen Verbindungsbeamten, Grenzschutzdatenbanken, Handelsregister, automatische Nummernschilderkennung usw.

Schnittstellen sollen auch zu “Strom- und der Wasserversorgungsunternehmen” eingerichtet werden. Die geplante Anbindung von “Telefon- und sonstigen Telekommunikationsunternehmen” lässt darauf schließen, dass auch der leichtere Zugriff auf abgehörte Telekommunikation geplant ist. Denn die Anlaufstellen können auch für die “Sofortgenehmigung” dringender Überwachungsmaßnahmen angepingt werden.

Nicht nur im föderalen System Deutschlands ist es problematisch, wenn die neuen “Single Points of Contact” über die “umfassendste nationale Zuständigkeit” verfügen sollen. Denn Polizei ist hierzulande Ländersache. Das hat man auch beim Rat der Europäischen Union bedacht und trägt einschränkend vor, nicht alle Leitlinien, Empfehlungen oder Beispiele seien “in jedem Mitgliedstaaten sinnvoll oder gar anwendbar”.

Zunächst sind die Leitlinien auch nicht bindend. Es könnte aber gut sein, dass in einigen Jahren eine Verordnung daraus wird.

0

by Matthias Monroy at July 09, 2014 05:17 PM

Störerhaftung: Freifunker klagen vor Berliner Amtsgerichten – Gesetzgeber bleibt am Zug

Foto: flickr/stk_ulm, CC-BY-SA 2.0

Die beiden Berliner Freifunk-Aktivisten Ralf Gerlich und Bianco Veigel haben vor den Amtsgerichten Neukölln und Lichtenberg Klage erhoben. Sie wollen gerichtlich feststellen lassen, dass sie nicht für mutmaßliches Filesharing durch unbekannte Nutzer ihrer Funknetze haften. Die beiden waren jeweils für angebliches Filesharing abgemahnt worden, das sie dadurch ermöglicht haben sollen, dass sie ihre WLANs bewusst nicht verschlüsseln, sondern der Öffentlichkeit frei zur Verfügung stellen.

Bei den Klagen wird es rechtlich vor allem darum gehen, ob das sog. Providerprivileg des § 8 Abs. 1 des Telemediengesetzes auch für “Nebenbei-Provider” wie die beiden Freifunker gilt. Zwar unterscheidet das Gesetz eigentlich nicht danach, ob jemand den Internet-Zugang gegen Entgelt oder gratis anbietet. Gleichwohl herrscht derzeit in Deutschland eine im internationalen Vergleich einmalige Rechtsunsicherheit. Zwar käme niemand auf den Gedanken, etwa die Telekom für Urheberrechtsverletzungen abzumahnen, die über ihre Access Points begangen werden. Anders sieht die Lage aber für “Nebenbei-Provider” wie die Freifunker oder auch Cafes und Hotels aus: Der Bundesgerichtshof hat 2010 in seiner (halbwegs) einschlägigen Entscheidung “Sommer unseres Lebens” zur Haftung von WLAN-Betreibern das Providerprivileg nicht einmal erwähnt. Daher ist rechtlich ungeklärt, ob sich auch Betreiber von WLANs auf diese Haftungsbefreiung berufen können, die nicht dem klassischen Bild des Providers entsprechen. Folge: In Deutschland herrscht vergleichsweise “Funkstille auf dem Bürgersteig”, während man z.B. in den USA dauernd auf offene Netze trifft, die freundliche Menschen der Allgemeinheit zur Verfügung stellen.

Vor diesem Hintergrund wäre ein positiver Ausgang der beiden Berliner Musterverfahren sehr erfreulich, um die vom Gesetz nicht gedeckte Diskriminierung von “Nebenbei-Providern” aus der Welt zu schaffen. Man sollte allerdings nicht aus dem Blick verlieren, dass sich das Problem “Störerhaftung” allein gerichtlich leider kaum lösen lassen wird. Aufgrund des Instanzenzugs in Zivilsachen dürften die beiden nun bei Amtsgerichten erhobenen Klagen kaum beim Bundesgerichtshof ankommen. Alleine der BGH könnte aber eine bundesweit maßgebliche Entscheidung fällen. Und selbst wenn der BGH mit dem Problem wieder befasst werden sollte, so ist doch sehr fraglich, ob er seine Linie korrigieren würde: Immerhin hat er alle bisherigen Chancen ungenutzt gelassen, die Störerhaftung für WLANs abzuschaffen.

Daher liegt der Ball trotz der beiden Berliner Verfahren weiter im Feld des Gesetzgebers. Der Verein Digitale Gesellschaft hat bereits 2012 einen Muster-Gesetzentwurf veröffentlicht, wie das Problem der Störerhaftung gelöst werden könnte. Die LINKE hatte auf dieser Grundlage einen eigenen Entwurf in den letzten Deutschen Bundestag eingebracht. In einer Anhörung des Unterausschusses Neue Medien im Mai 2013 äußerten sich die angehörten Experten durchweg positiv dazu. Es bleibt zu hoffen, dass der jüngst angekündigte Gesetzentwurf aus dem Bundeswirtschaftsministerium die Störerhaftung für "Nebenbei-Provider" ebenso konsequent abschaffen wird wie es der Text der Digiges vorsieht. Leider könnte hier aber Unheil drohen: Die Süddeutsche Zeitung berichtet, dass das Wirtschaftsministerium das Providerprivileg nur für kommerzielle "Nebenbei-Provider" wie Cafes und Hotels klarstellen möchte. Damit stünden die nicht kommerziellen Freifunker endgültig im Regen, denn im Umkehrschluss würde der Gesetzentwurf dann wohl zugleich klarstellen, dass das Providerprivileg für sie tatsächlich nicht gilt. Die Digitale Gesellschaft forderte daher klarzustellen, dass die Störerhaftung keinen WLAN-Betreiber trifft. Letztlich wird das am genauen Wortlaut des Gesetzes hängen. Falls also jemand den Gesetzentwurf zufällig zur Hand hat …

0

by @vieuxrenard at July 09, 2014 03:19 PM

Recherche zeigt: Nur Industrie redet mit EU-Kommission über Netzpolitik bei TTIP

Das Corporate Europe Observatory (CEO) veröffentlichte gestern Daten darüber, woher eigentlich die meisten Lobbyisten in den TTIP-Verhandlungen kommen. Die Lobby-kritische Organisation recherchiert seit einiger Zeit über das geplante Freihandelsabkommen und veröffentlichte Ende vergangenen Jahres bereits die PR-Strategie der EU-Kommission, wie das Abkommen am besten der Öffentlichkeit verkauft werden solle).

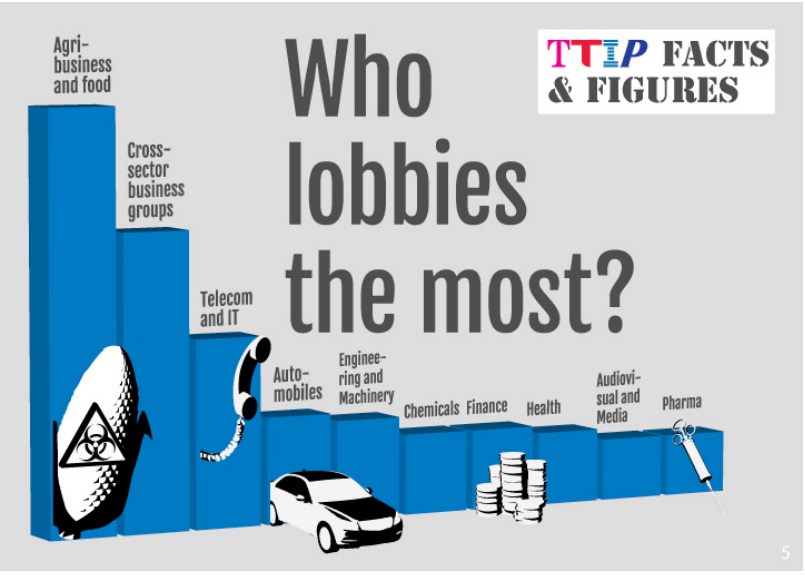
Um an Daten für die statistische Auswertung des Lobbyausmaßes zu gelangen, arbeiteten sie sich durch Einsendungen zu öffentlichen Konsultationen der EU-Kommission, Teilnehmerlisten von TTIP-Dialog-Events und Informationen über geheime Treffen mit der EU-Kommission, die sie über Informationszugangsanfragen erhielten. Obwohl diese Daten nur den Zeitraum von Anfang 2012 bis April 2013 abdecken, sich ausschließlich auf die federführende Generaldirektion 'Handel' beziehen und die Intensität der Treffen nicht mit einbeziehen, zeichnen sie doch ein deutliches Bild der Lobbylandschaft in der EU-Kommission noch vor der stärkeren gesellschaftlichen Aufmerksamkeit und dem öffentlichen Gegenwind für TTIP.

Vorrangig Industrievertreter, kaum öffentliche Interessen

Auffällig beim Betrachten der Ergebnisse ist die überproportionale Präsenz von privatwirtschaftlichen Lobbyverbänden gegenüber Vertretern öffentlichen Interesses. Von 560 gezählten Begegnungen waren nur 4% Vertreter öffentlicher Interessen wie Verbraucher- oder Umweltschutz. Der Rest entfiel auf Wirtschaftsvertreter.

Die Daten prangern auch das Transparenzproblem der EU bezüglich des Lobbyismus an: Mehr als ein Drittel der aufgezeichneten Verbände ist nicht in dem (freiwilligen) Transparenzregister der EU verzeichnet, und diejenigen, die dort zu finden sind, hüllen sich über ihre Themen in Stillschweigen, die wenigsten bringen sich direkt mit TTIP in Verbindung.

Aus unserer Sicht spannend sind aber vor allem die Branchen, die die größten Lobbyanstrengungen aufbringen: Ungeschlagen ist die Agrarwirtschaft und Ernährungsbranche, mit Unternehmen wie Nestlé und Coca-Cola, auf die 113 der 560 Treffen entfallen. Die IT-Branche und die Urheberrechtsindustrie haben allerdings auch nicht geschlafen:



Wer lobbyiert am meisten? | Grafik von CEO

Als Drittstärkste neben den branchenübergreifenden Wirtschaftsverbänden machten sie sich für ihre jeweiligen Interessen stark. Zusammen mit diversen Vertretern aus der Audiovisuellen bzw. Medienbranche sind sie für uns aus netzpolitischer Sicht interessant. Wir haben uns die Datengrundlage von CEO einmal angesehen und die netzpolitisch-relevanten Firmen und Verbände herausgezogen, um sie hier zu veröffentlichen:

298 Lobbygruppen sind insgesamt aufgelistet, von diesen sind 51 von netzpolitischem Interesse. Nur eine dieser 51 – der Transatlantic Consumer Dialogue (TACD) – gehört zu den "Guten", setzt sich also für Verbraucherrechte ein. Die restlichen hier aufgelisteten Unternehmen, etwa ein Sechstel der insgesamt involvierten Gruppen, lobbyieren für deren eigene wirtschaftlichen Interessen. Organisationen wie die US Chamber of Commerce haben wir trotz vordergründig mangelndem IT-Bezug aufgenommen, weil Unternehmen wie Microsoft in der Vergangenheit über diese Bande gespielt haben, um ihre Interessen durchzusetzen.

Liste der Netzpolitik-Lobby

US Chamber of Commerce
Digital Europe
European Telecommunications Network Operators' Association (ETNO)
BT Group
Nokia
Deutsche Post DHL
International Confederation of Music Publishers
The Association of European Chambers of Commerce and Industry
Ericsson
International Federation of Reproduction Rights
IFPI Representing recording industry worldwide
Ebay Inc.
IBM
Mediaset (Italian Media Company)
News Corp
RTL Group
Walt Disney
European Broadcasting Union
Federation of European Publishers
Motion Picture Association of America
National Music Publishers Association in the US
European Coordination of Independent Producers
Record Industry Association of America (RIAA)
International Trademark Association
Danish Chamber of Commerce
IP Federation
American Chamber of Commerce France
American Chamber of Commerce in Germany
Siemens
Zentralverband Elektrotechnik- und Elektronikindustrie e.V.
Transatlantic Consumer Dialogue
European Patent Office
Google
Blackberry
Inmarsat Global Ltd
Microsoft
Qualcomm
Samsung
Intel Corporation
Texas Instruments
UVAX Concepts
Skynet
Deutsche Telekom
France Telecom
Huawei
SES – Global Satellite Service Providers
Telefónica
Telenor
Verizon
Vodafone
TechAmerica Europe
Business Software Alliance
Information Technology Industry Council

0

by Elisabeth Pohl at July 09, 2014 02:09 PM

How-To Analyze Everyone – Teil VIII: Browser-Fingerprints und Informationskrümel ohne Cookies

Du hast alle Cookies deaktiviert? Und das “Do Not Track”-Häkchen gesetzt? Nutzt einen Proxy? Und du denkst jetzt ist es ziemlich schwierig, dich im Internet zu tracken? Leider wiegst du dich da in falscher Sicherheit, denn nicht nur ein Cookie kann verraten, wer du bist. Auch die Eigenschaften, die dein Browser über sich und dein System verrät, können ein ziemlich einzigartiges Identifikationsmerkmal sein. Genauso wie ein selten vorkommender Name es entbehrlich macht, auch noch Adresse/Geburtsort/Geburtsdatum einer Person zu prüfen, um festzustellen, um wen es sich handelt, kann ein einzigartiger Browser-Fingerprint es leicht möglich machen, einen Nutzer zu tracken – ganz ohne Cookies, das Einfügen von IDs in URLs, HTML-Formulare oder andere klassische Tracking-Mechanismen.

Das ist für diejenigen praktisch,die uns gezielt mit personalisierter Werbung beglücken wollen, auch wenn wir offensichtlich bereits Verkehrungen getroffen haben, damit genau das nicht passiert. Denn natürlich ist es aus kommerzieller Sicht ärgerlich, dass mittlerweile viele Nutzer Cookies blocken oder zumindest regelmäßig löschen. Wie das in Werbe-Sprech aussieht, kann man sich auf den Seiten von Zanox anschauen, einem großen Marketing- und ECommerce-Dienstleister:

> Mit „zanox TPV Fingerprint Tracking“ (TPV – True Post View) erweitern wir unsere marktführende Tracking-Technologie mit einer passiven Lösung für das Tracking von Display-Werbemitteln. Das „zanox TPV Fingerprint Tracking“ basiert nicht auf dem Einsatz von Cookies und bietet damit eine präzise und zuverlässige Alternative, wenn Cookies gelöscht, deaktiviert oder mittels entsprechender Browser-Einstellung blockiert werden. [...] Das zanox Tracking-System ist so konzipiert und dimensioniert, dass es alle Aktionen in Echtzeit verarbeiten kann und jederzeit unterhalb der maximal möglichen Arbeitslast bleibt. Derzeit bedient die zanox Tracking-Architektur etwa 600 Millionen Ad-Impressions, 50 Millionen Klicks und mehr als zwei Millionen Kunden-Transaktionen pro Tag.

Gleichzeitig demonstriert uns eine kleinen Infografik schön das Ziel des Ganzen, nämlich wie unsere persönlichen Daten ganz einfach zu Geld werden:

via blog.zanox.com

Aber zuerst einmal wollen wir uns anschauen, wie so ein Browser-Fingerprint eigentlich aussieht und warum er uns so gut identifizieren kann.

Welchen Fingerabdruck hat mein Browser?

Einfache Wege sich anzuschauen, welche Charakteristika der eigene Browser dem Internet offenbart, bietet zum Beispiel die Electronic Frontier Foundation mit Panopticlick. Hat man nicht bereits Maßnahmen zur Minimierung der eigenen Verfolgbarkeit getroffen, bekommt man im Normalfall das recht ernüchternde Ergebnis, dass der eigene Browser unter den mehreren Millionen bislang getesteten einzigartig ist. Betriebssystem, installierte Schriftarten, Browserplugins und vieles mehr posaunen wir beim Surfen im Internet bereitwillig in die Welt hinaus. Zusätzlich dazu, was man preisgibt, zeigt Panopticlick außerdem an, wie verbretet die einzelnen Eigenschaften unter den Browsern sind, die bereits erfasst wurden. Oder anders ausgedrückt – wieviele Bits an Information man zur Identifikation bereitstellt. Je einzigartiger und detaillierter beispielsweise die “User Agent”-Angabe ist, die Angaben zu Browser, Betriebssystem und teilweise weiteren Infos wie Hardwareplattform bietet, desto mehr Informationsgehalt trägt diese Auskunft.

Browser Characteristic	bits of identifying information	one in *x* browsers have this value	value
User Agent	12.56	6023.58	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Ubuntu Chromium/34.0.1847.116 Chrome/34.0.1847.116 Safari/537.36
HTTP_ACCEPT Headers	10.82	1802.73	text/html, */* gzip,deflate,sdch en-US,en;q=0.8,de;q=0.6

Ein ganz kurzer Ausflug in die Informationstheorie

“Bits of identifying information” – klingt erstmal kryptisch. Was heißt das konkret: 12,56 bits, die durch den User Agent bereitstehen, um mich zu identifizieren? Das Maß des Informationsgehalts einer Angabe in Bit formalisiert, wie viel “Überraschung” eine Nachricht enthält. Das heißt: Es zählt nicht die Menge an Information, sondern wieviel Neuigkeitswert diese bietet, wie wahrscheinlich ihr Auftreten ist. Mathematiker würden das so sagen:

$$I(p_x) = \log_a \left(\frac{1}{p_x} \right)$$

Bevor wir uns abschrecken lassen, betrachten wir ein einfaches Beispiel. Nehmen wir den Fall an, es gäbe nur Männer und Frauen auf der Welt und davon jeweils genau 50%, also ist die Wahrscheinlichkeit *p* 0,5. Dabei sind die möglichen Zustände, die Auftreten können – *a* – genau 2. In die Formel eingesetzt:

$$I(p_x) = \log_2 \left(\frac{1}{0,5} \right) = 1$$

Die Information, dass eine Person weiblich ist, enthält also genau 1 bit Information. Logisch, denn es gibt zwei Zustände und definiert man männlich als “0″ und weiblich als “1″ hat man alles abgedeckt.

Gibt es mehr Auswahlmöglichkeiten, also mehr Unsicherheit, wie das Ergebnis aussieht, steigt auch der Informationsgehalt. Schauen wir

uns das Beispiel des Browsers an. Die Wahrscheinlichkeit, dass ein anderer Browser den gleichen "User Agent"-String schickt ist laut Tabelle 1/6023,58, demnach in etwa 0,0166%. Der Informationsgehalt beträgt also, wenn wir als mögliche Zustände "hat diesen User Agent" oder "hat einen anderen User Agent" annehmen:

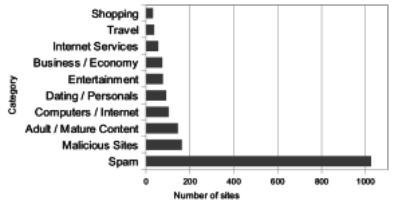
$$I(p_x) = \log_2\left(\frac{1}{0,0166}\right) = 12,5564$$

Damit lässt sich hoffentlich etwas besser verstehen, wie die Zahlen zustande kommen, die in der Auswertung angegeben sind.

Die EFF hat bei der Auswertung der Ergebnisse von Panopticlick übrigens festgestellt, dass Browser, die Flash und Java unterstützen, im Durchschnitt mindestens 18,8 bits Informationen bereitstellen, 94,2% dieser Browser waren in der Testmenge einzigartig. Henning Tillmann, der Browser-Fingerprints in seiner Diplomarbeit untersucht hat, kam außerdem zum Ergebnis, dass es bei 60 % der Nutzer über einen längeren Zeitraum zu keinerlei Veränderungen an ihrem Fingerprint kommt, bei 90% hatten sich höchstens drei Merkmale verändert.

Kommerzielle Tracking-Software kann noch mehr

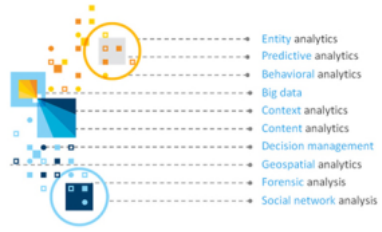
Wer glaubt, die Informationen, die Panopticlick auswertet, wären schon genug, sollte sich bewusst machen, dass die Firmen, deren Tagesgeschäft das Tracking darstellt, sich noch weitaus mehr einfallen lassen, um Detailinformationen zu bekommen. Forscher der KU Leuven und der University of California haben drei kommerzielle Fingerprinting-Anbieter untersucht und konnten dabei einige Taktiken der "Cookieless Monsters" rekonstruieren. Die Haupterkenntnis: Die professionellen Tracker schaffen es, noch weit mehr Informationen zu ermitteln. Dabei wurden vor allem Flash-Plugins genutzt. Die senden als Plattformangabe nicht "nur" wie etwa Firefox das Betriebssystem mit Hardwarearchitektur, sondern noch dazu die genaue Kernelversion – was nicht nur beim Tracking hilft, sondern auch, wenn man gezielt Schwachstellen in bestimmten Systemversionen missbrauchen will. Ein weitere Lücke, die Flash in die die digitale Schutzmauer eines Nutzers reißen kann ist die Umgehung von IP-Adressen-Anonymisierung bei der Nutzung von HTTP-Proxies, da ein Flash-Plugin in der Lage ist, die Umleitung zu ignorieren und somit einem Tracker die wahre IP des Nutzers mitteilt.



Interessant ist nicht nur, wie die Fingerprinting-Skripts arbeiten, sondern auch, wer sie nutzt. Die intuitive Vermutung fällt auf Shopping-Seiten, eine Statistik aus der obigen Studie kommt zu anderen Ergebnissen. Ganz weit vorn liegen Spam- und Schadseiten – womit man wieder bei genauen Infos zum Ausnutzen von Sicherheitslücken wäre.

Doch wie immer gibt es nicht nur eine Seite der Medaille, sondern es ergeben sich auch vermeintlich nützliche Anwendungen, bei denen Browser-Fingerprinting eine Rolle spielt.

Patentierte Betrugserkennung über den Browser



IBM hat ein System patentieren lassen, das die Möglichkeit bieten soll, Online-Betrug zu erkennen bevor er überhaupt entsteht. Dafür wurden Unmengen Verhaltensdaten vor dem Ausführen von Transaktionen wie Online-Bestellungen und Zahlvorgängen gesammelt. Die erfassten Informationen umspannen unter anderem das Navigationsverhalten des Nutzers – arbeitet er mit der Maus oder den Pfeiltasten, wohin klickt er am häufigsten -, den besagten Browser-Fingerprint und eine Statistik über gewöhnliche Anmeldezeiten und Orte des Nutzers. Alles plausibel, aber entsprechend der nebenstehenden Infografik von der IBM-Seite gehören auch Social-Media-Daten und "Big Data" allgemein zu den Informationsquellen. Kurzum: Alles, was man bekommen kann, wird herangezogen, um das Normalverhalten des Nutzers zu modellieren. Weicht er vom über ihn bekannten Standard ab, tritt eine weitere Authentikationsstufe in Kraft bei der er beweisen muss, dass er wirklich die vorgegebene Person ist. Das können Captchas sein, aber auch andere Two-Factor-Authentication-Methoden wie SMS-Codes.

Neu ist die Idee nicht, ein früheres IBM-Patent stammt bereits aus dem Jahr 2007. Und ähnlich ist auch das Informieren und Blocken von Accounts bei "ungewöhnlichen" Aktivitäten, das bereits jetzt von Google und Co. genutzt wird. Nur dass dann vielleicht schon der Zugang zum Mailpostfach geblockt wird, wenn die linke Hand statt der rechten zum Klicken benutzt wird, weil mit der anderen gerade eine Kaffeetasse gehalten wird oder man morgens um fünf ausnahmsweise spontan eine MP3 erwerben will, weil man gerade noch einen furchtbaren Ohrwurm hat, nachdem man vom Tanzen kommt. Und nicht, weil ein Anmelde-Versuch von einem bisher unbesuchten Ort stattfindet.

Was tun?

Klar ist: Das Missbrauchspotential von Browser-Fingerprints ist hoch und man sollte sich darum Gedanken machen, wie man sich bestmöglich schützen kann. Eine Patentlösung können wir nicht geben, aber ein paar Hinweise, wie man es den Trackern zumindest schwerer machen kann:

Sei Durchschnitt. Mit einem aktuellen Browser auf einem Mainstream-Betriebssystem kann man leichter in der Masse untergehen als das mit einem antiquierten Internet Explorer. Alternativ zum Browser und System könnte man auch den User Agent ändern. Der Browser sendet dann andere Informationen an die Webseite als eigentlich zutreffend. Geht zum Beispiel mit dem User Agent Switcher für Firefox, ist aber nicht zwingend sinnvoll. Denn wenn von einer einzelnen IP ständig andere User Agent Angaben gesendet werden, fällt das a) sowieso auf und b) landet man schnell automatisch als Spambot-Verdächtiger auf Blocklisten.

JavaScript und Flash deaktivieren. Vermeidet man die Nutzung von JavaScript und Flash, können keine Merkmale mehr aktiv vom Browser erfragt werden. Also keine Informationen mehr, welche Plugins genutzt werden, welche System-Schriftarten installiert sind u.v.m. Dafür gibt es unter anderem das beliebte NoScript, das auch Einzelentscheidungen ermöglicht, welche Seiten/Skripte geblockt werden und welche nicht. Wie stark sich das Ausschalten von JavaScript auf die Identifizierung auswirkt, kann man mit Panopticlick schön beobachten. In einer Testumgebung sank die indentifizierende Information von 20,44 bits auf 14,4 bits.

Vorher:

Browser Characteristic	bits of identifying information	one in *x* browsers have this value	value
User Agent	10.71	1674.45	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:29.0) Gecko/20100101 Firefox/29.0
HTTP_ACCEPT Headers	4.21	18.53	text/html, */* gzip, deflate en-US,en;q=0.5
Browser Plugin Details	13.93	15579.16	Plugin 0: DivX® Web Player; DivX Web Player version 1.4.0.233; libtotem-mully-plugin.so; (AVI video; video/divx; divx). Plugin 1: QuickTime Plug-in 7.6.6; The Videos 3.10.1 plugin handles video and audio streams.; libtotem-narrowspace-plugin.so; (QuickTime video; video/quicktime; mov) (MPEG-4 video; video/mp4; mp4) (MacPaint Bitmap image; image/x-macpaint; pntg) (Macintosh Quickdraw/PICT drawing; image/x-quicktime; pict, pict1, pict2) (MPEG-4 video; video/x-m4v; m4v) (HTTP Live Streaming playlist; application/vnd.apple.mpegurl; m3u8). Plugin 2: Shockwave Flash; Shockwave Flash 11.2 r202; libflashplayer.so; (Shockwave Flash; application/x-shockwave-flash; swf) (FutureSplash Player; application/futuresplash; spl). Plugin 3: VLC Multimedia Plugin (compatible Videos 3.10.1); The Videos 3.10.1 plugin handles video and audio streams.; libtotem-cone-plugin.so; (VLC Multimedia Plugin; application/x-vlc-plugin;) (VLC Multimedia Plugin; application/vlc;) (VLC Multimedia Plugin; video/x-google-vlc-plugin;) (Ogg multimedia file; application/x-ogg; ogg) (Ogg multimedia file; application/ogg; ogg) (Ogg Audio; audio/ogg; oga) (Ogg Audio; audio/x-ogg; ogg) (Ogg Vorbis audio; audio/x-vorbis+ogg; ogg) (Ogg Video; video/ogg; ogv) (Ogg Video; video/x-ogg; ogg) (Ogg Theora video; video/x-theora+ogg; ogg) (Annodex exchange format; application/annodex; anx) (Annodex Audio; audio/annodex; axa) (Annodex Video; video/annodex; axv) (MPEG video; video/mpeg; mpg, mpeg, mpe) (WAV audio; audio/wav; wav) (WAV audio; audio/x-wav; wav) (MP3 audio; audio/mpeg; mp3) (NullSoft video; application/x-nsv-vp3-mp3; nsv) (Flash video; video/flv; flv) (WebM video; video/webm; webm) (Videos multimedia plugin; application/x-totem-plugin;) (MIDI audio; audio/midi; mid, midi). Plugin 4: Windows Media Player Plug-in 10 (compatible; Videos); The Videos 3.10.1 plugin handles video and audio streams.; libtotem-gmp-plugin.so; (AVI

Nachher:

Browser Characteristic	bits of identifying information	one in *x* browsers have this value	value
User Agent	10.71	1675.77	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:29.0) Gecko/20100101 Firefox/29.0
HTTP_ACCEPT Headers	4.97	31.3	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 gzip, deflate en-US,en;q=0.5
Browser Plugin Details	1.74	3.35	no javascript
Time Zone	1.74	3.34	no javascript
Screen Size and Color Depth	1.74	3.34	no javascript
System Fonts	1.74	3.34	no javascript
Are Cookies Enabled?	1.95	3.88	No
Limited supercookie test	1.74	3.34	no javascript

Nutze Tor. Tor anonymisiert nicht nur deine IP-Adresse, sondern der Tor-Browser schickt auch eine einheitliche User-Agent-Angabe mit blockt standardmäßig Java- und Flashanwendungen.

Nachdenken. Auch wer alle technischen Maßnahmen ergreift muss sich trotzdem noch bewusst machen, dass er auch durch unachtsames Verhalten schnell Datenspuren hinterlassen kann. Wer sich über Tor bei einem Mailanbieter mit Klarnamen anmeldet ist diesem gegenüber genauso wenig anonym wie mit einer direkten Verbindung…

Fazit: **Es ist kompliziert**. Nicht nur der einzelne Nutzer sorgt sich um Browser-Fingerprints, auch im W3C beschäftigt man sich damit, wie man vermeiden kann, dass solches Fingerprinting erst möglich wird. Eine Präsentation vom Technical Plenary / Advisory Committee Meeting des W3C 2012 mit dem Titel "Is preventing browser fingerprinting a lost cause?" zeigt deutlich, wo das Problem liegt:

Internetprotokolle wurden weitgehend entworfen ohne die potentielle Bedrohung der Privatsphäre von Nutzern im Blick zu haben. Dementsprechend nutzen sie eine Menge Daten, die vielleicht vermieden werden könnten und so mehr Möglichkeiten zum anonymen Internetnutzung lassen würden. Und es ist wie immer schwer, nachträglich Maßnahmen zum Schutz selbiger im Nachhinein einzubauen. Notwendig wären also neue Protokolle, die Fingerprinting vermeiden. Womit wir auch beim generellen Vermeiden von Metadaten wären.

Ohne Browser-Fingerprints alles gut?

Sind wir endlich anonym, wenn wir es geschafft haben, alle Cookies zu blocken, verräterische Flash-Applikationen zu umgehen, JavaScript auszuschalten und noch jemand Protokolle entwirft, die unsere Browser-Fingerprints gar nicht erst aufnehmen und zum Beispiel keine User-Agent-Infos mehr in die Welt senden? Nein, natürlich nicht. Denn es wird wohl immer etwas zum Identifizieren geben. Zum Beispiel das Verhalten des Browsers und den Charakteristiken der Grafikkarte beim Rendern von Pixeln auf einem HTML5-Canvas-Element. Und die nächste Sicherheitslücke ist

Bisher gab es in dieser Reihe:

- How-To Analyze Everyone – Teil I: Basics der Handyortung
- How-To Analyze Everyone – Teil II: Wie findest du eigentlich Zombiefilme?
- How-To Analyze Everyone – Teil III: Ich weiß, wo du heute abend sein wirst
- How-To Analyze Everyone – Teil IV: Kunden, die diese Feueraxt gekauft haben, mögen Zombiefilme
- How-To Analyze Everyone – Teil V: Der Algorithmus weiß besser als Du, wer zu Dir passt
- How-To Analyze Everyone – Teil VI: Neurotisch? Extrovertiert? Dein Provider könnte es wissen
- How-To Analyze Everyone – Teil VII: Zeig mir dein Gesicht

0

by Anna Biselli at July 09, 2014 12:55 PM

BPjM-Leak: Warum wir erstmals einen Link aus unserer Berichterstattung entfernen. Oder: Verbreiten wir Kinderpornografie? (Updates)

Wir so anno 2009 gegen Zensursula: “Löschen statt Sperren!”

Das erste Mal in unseren fast zehn Jahren an Berichterstattung haben wir einen Link aus einem Beitrag entfernt. Die Kommission für Jugendmedienschutz hat gedroht, uns wegen der “Zugänglichmachung von Kinderpornografie” anzuzeigen. Anlass ist unser Bericht über die veröffentlichte Sperrliste indizierter Webseiten der Bundesprüfstelle.

Gestern haben wir darüber berichtet, dass die geheime Liste in Deutschland indizierter Webseiten veröffentlicht wurde. Fast die Hälfte der darin enthaltenen URLs existiert gar nicht mehr, andere sind typische Fälle von Overblocking. Mittlerweile hat die Bundesprüfstelle für jugendgefährdende Medien (BPjM) die Echtheit der Liste in einer Pressemitteilung bestätigt:

> Am Dienstag, 8. Juli 2014, erhielt die Bundesprüfstelle Kenntnis darüber, dass die im sog. BPjM-Modul enthaltenen URLs im Klartext auf einer Internetplattform veröffentlicht wurden.
> […]
> Die erfolgte Veröffentlichung der indizierten URLs läuft damit den Zielsetzungen des Jugendschutzes eklatant zuwider. Die BPjM weist darauf hin, dass die veröffentlichte URL-Liste auch solche Angebote enthält, deren bloßer Aufruf eine Strafverfolgung nach sich ziehen kann. Die BPjM hat die zuständige Aufsicht über den Jugendschutz im Internet, die Kommission für Jugendmedienschutz (KJM), das Bundeskriminalamt sowie die Staatsanwaltschaft über den Vorgang informiert und Strafanzeige gegen Unbekannt gestellt.

Wenige Stunden nach unserer Berichterstattung rief eine Vertreterin der Kommission für Jugendmedienschutz der Landesmedienanstalten (KJM) bei uns an. Wir sollten den Link auf den “BPjM-Leak” beim Freehoster Neocities entfernen. Manche der (über 3.000) URLs auf der Seite enthalten demnach strafbares Material nach § 184b Strafgesetzbuch, vulgo: “kinderpornographische Schriften”. Unser Link wäre “Zugänglichmachung” von “Kinderpornografie”.

Das hat uns ehrlich gesagt überrascht. Dass das Veröffentlichen der Liste selbst laut Jugendschutzgesetz strafbar ist, war uns bekannt. Das haben wir nicht getan. Obwohl man die Meinung vertreten könnte, dass die BPjM die Liste selbst öffentlich macht und verbreitet – man muss lediglich etwas technischen Aufwand betreiben, die URLs zu errechnen, wie die Leakerin eindrücklich beschrieben hat.

Haftung für Hyperlinks?

Aber dass man uns **Zugänglichmachung** strafbarer Inhalte vorwirft, weil wir im Rahmen unserer Berichterstattung auf eine Webseite linken, die wiederum URLs als nicht-verlinkten Text enthält, hat uns doch etwas verwundert. Haben wir nicht jahrelang gegen Linkhaftung gekämpft und immer wieder gewonnen, wie heise online und Alvar Freude zeigen?

Wir machen uns hier nicht die Inhalte der Seite BPjM-Leak zu eigen. Und erst recht nicht die der URLs in der Sperrliste. Im Gegensatz, wir übersetzen diesen Text des Hackers:

> Die meisten Einträge der liste können als eine der folgenden Kategorien eingestuft werden: normale Pornografie, Tierpornografie, Kinder-/Jugendpornografie, Suizid, Nazis oder Anorexie.

Zudem haben wir fünf Jahre lang im Arbeitskreis gegen Internet-Sperren und Zensur (AK Zensur) gegen Netz-Sperren gekämpft. Falls es eindeutig strafbare Inhalte wie Missbrauchsdokumentation im Internet gibt, müssen die an der Quelle entfernt und strafrechtlich verfolgt werden. Löschen statt Sperren. Wir haben den Kampf gewonnen, das Zugangserschwerungsgesetz wurde zurückgenommen. (Ich hatte damals meine Master-Arbeit darüber geschrieben.)

Löschen statt Sperren!

Auch die BPjM selbst sagt, dass dieses Verfahren funktioniert, wie ihr Jahresbericht Löschung von kinderpornographischen Inhalten zeigt:

> Die Zusammenarbeit von Beschwerdestellen und BKA zur Verbesserung der Löschung kinderpornografischer Inhalte im WWW hat sich bewährt.
> […]
> Dennoch funktioniert die Löschung kinderpornographischer Inhalte sehr gut.

Falls sich auf der nun veröffentlichten Liste wirklich Seiten mit strafbarem Material nach § 184b befinden, muss man sich fragen, warum diese erfolgreiche Löschung da nicht durchgeführt wurde und stattdessen mal wieder nur ein Vorhang vor den Ort des Verbrechens gehängt wird, damit die Seiten nicht in Suchmaschinen angezeigt werden und von wenigen Routern, auf denen die Filter-Liste aktiviert wurde, gesperrt wird. Statt das Übel an der Wurzel zu packen.

Ganz besonders stört uns, dass wir auf die Seite nicht einfach linken, um die Sperrliste zu bewerben oder uns die Inhalte zu eigen zu machen, sondern weil wir seit Jahren über das Thema Netz-Sperren und Filter-Listen berichten. Und bei Berichterstattung im Internet verlinken wir nunmal auf die Originalquelle, alles andere ist unseriös. Auch andere Medien wie heise online und chip.de haben (zum

Zeitpunkt dieses Postings) den Link gesetzt. (Mal abgesehen von über 100 Tweets).

Zwei Juristen, drei Meinungen

Politisches Handeln ist aber anders als die Gesetzeslage. Also haben wir mal ein paar Anwälte angefragt.

Thomas Stadler, Fachanwalt für IT- Recht, sieht das ähnlich wie wir. Zwar gibt es "viele Punkte zu prüfen", deswegen wäre er vorsichtig. Aber wir haben ein Berichterstattungsprivileg. Wenn wir über den Leak berichten, sollte ein Link auf die Seite des Leakers von diesem Privileg gedeckt sein. Zudem verlinken wir die angeblich strafbaren Inhalte gar nicht direkt, sondern wir verlinken auf die Leak-Webseite, die wiederrum die URLs als nicht-verlinkten Text enthält. Das ist wesentlich schwächer als ein direkter Link. Stadler: "Ich halte es durchaus vertretbar, zu sagen, dass ihr euch nicht strafbar gemacht habt."

Ein weiterer Fachanwalt für IT-Recht sieht das kritischer. Man könnte der Rechtsauffassung der KJM folgen: "Denn durch den Link wird, neutral betrachtet, der Zugang zu Kinderpornografie (mal unterstellt es gibt tatsächlich solche Seiten unter den Links) vereinfacht bzw. ermöglicht." Die Vorschriften nach § 184b Strafgesetzbuch sind da recht eindeutig. Das Verfahren Heise vs. Musikindustrie war Zivilrecht, nicht Strafrecht. "Die wenigen Urteile zu Strafrecht und Links stellten darauf ab, ob der Verlinkende erkennen konnte, dass er auf strafrechtlich relevante Inhalte verweist. Das dürfte ja hier eher unstreitig sein."

Thorsten Feldmann, Fachanwalt für Urheber- und Medienrecht, hingegen gibt uns wieder Recht:

> Die einschlägigen Vorschriften des JuSchG und des JMStV tolerieren Veröffentlichungen auch von Teil C und D der Liste, wenn diese nicht zu Werbezwecken erfolgt. Für die Strafbarkeit wird also eine qualifizierte Form der Veröffentlichung verlangt. Nach der gesetzgeberischen Wertung soll die schlichte Veröffentlichung der gesamten Liste zulässig, auch wenn dadurch etwa nachvollziehbar wird, wo die rechtswidrigen Inhalte auffindbar sind. Diese Wertung muss man auch bei der Frage der Zugänglichmachung im Sinne des § 184 b StGB beachten.
>
> Darüber hinaus würde euch (spätestens) die Meinungs- und Pressefreiheit die Veröffentlichung gestatten.

Sönke Hilbrans, Strafverteidiger und Fachanwalt für Strafrecht meint:

> Ob ein Link, zumal wenn er den Download des strafbaren Inhalts gar nicht direkt ermöglicht, überhaupt als Zugänglichmachung im strafrechtlichen Sinne gelten darf, ist schon mehr als fraglich. Die Rechtsprechung hat sich dazu bisher aus guten Gründen nicht durchgerungen, im Gegenteil: wer den inkriminierten Inhalt nicht selbst speichert und anbietet, macht ihn in der Regel auch nicht zugänglich. "Zugänglich" ist eben nicht schon "auffindbar". Auf das Argument mit der Meinungsfreiheit kommt es daher zunächst gar nicht an. Das heißt freilich nicht, dass ihr nicht damit rechnen müsst, dass gegen euch ermittelt wird: auch experimentelle Rechtsansichten können überzeugte Strafverfolger finden.

Zu großes Risiko

Tolle Aussichten. Aber selbst wenn uns neun von zehn Anwälten Recht geben würden, brächte uns das wenig. Recht haben und Recht kriegen ist leider nicht das selbe. Die KJM droht uns mit Strafanzeige – wegen Verbreitung von Kinderpornografie. Das ist ein schwerwiegender Vorwurf, der für mich als Autor des Beitrags und Markus als Verantwortlichen von netzpolitik.org nicht nur jahrelangen Stress durch Gerichtsverfahren, sondern im schlimmsten Fall auch eine Verurteilung und persönliche Haftung für eine der unangenehmsten Straftaten bedeuten könnte. Achja, und bis zu einer halben Millionen Euro Strafzahlungen – zusätzlich zu den Anwaltskosten. Und es ist durchaus möglich, dass Staatsanwält/innen und Gerichte das anders sehen als wir – und uns verurteilen.

Aus diesen Gründen haben wir – entgegen unserer Überzeugung – beschlossen, den Link im Original-Beitrag herauszunehmen. Das hält natürlich keine einzige Person davon ab, die Seite trotzdem zu finden.

Ich hoffe, ihr könnt diese Entscheidung nachvollziehen.

Achja, wir sind mittlerweile mit dem Hacker/der Hackerin in Kontakt und werden über seine oder ihre Sicht der Dinge berichten, sobald wir Antworten dazu haben. Ganz besonders ärgert uns, das wir seit über 24 Stunden auch versuchen, die BPjM zu kontaktieren. Weder per E-Mail noch auf unsere Anrufe wurde jemals reagiert – nur einmal hieß es: "Die Antwort kommt in der nächsten Stunde." Das war gestern Mittag.

Update: Heise hat den Link jetzt auch rausgenommen:

> Die Redaktion von heise online hat nach langer Diskussion beschlossen, den ursprünglich in diesem Beitrag enthaltenen Link auf die Seite #BPjMleak zu entfernen. Zwar sind wir nach wie vor der Ansicht, dass es ein großes öffentliches Interesse an der Bereitstellung der auf der Seite enthaltenen Hintergrund-Informationen zum Ablauf des Hacks besteht. Auf der anderen Seite besteht für unsere Mitarbeiter persönlich aufgrund der Veröffentlichung des Beitrags wegen der ebenfalls auf der Seite veröffentlichten Link-Liste ein Risiko strafrechtlicher Ermittlungen wegen der Verbreitung von Kinderpornografie und anderer Delikte. Wir haben uns im Interesse der Kollegen entschieden, dieses Risiko nicht einzugehen.

Update 2: Auch Chip Online hat den Link mittlerweile entfernt, ebenso Blogger wie Max.

Update 3: Thomas Stadler hat jetzt nochmal etwas ausführlicher gebloggt:

> Der konkrete Fall liegt allerdings anders, eine (direkte) Verlinkung ist nicht gegeben. Netzpolitik.org hat keine Links auf indizierte Websites gesetzt, sondern lediglich auf eine andere Seite verlinkt, auf der die Liste mit indizierten Websites veröffentlicht worden war. Aber auch auf dieser Seite sind keine Links vorhanden, sondern nur eine Auflistung der URLs in Textform. Die Frage ist also, ob der bloße Hinweis auf eine im Netz befindliche Veröffentlichung einer Liste in reiner Texform bereits strafrechtlich relevant sein kann. Insoweit ist außerdem besonders zu berücksichtigen, dass der Hinweis im Rahmen der Berichterstattung erfolgte, weshalb zusätzlich eine Würdigung im Lichte von Art. 5 GG geboten ist. Ein solches Verhalten kann deshalb auch bei großzügiger Auslegung nicht mehr als öffentliche Zugänglichmachung von strafbaren Inhalten angesehen werden.

Update 4: Udo Vetter, Fachanwalt für Strafrecht, hat sich auch dazu geäußert:

> Danach ist es durchaus riskant, direkt auf strafbare Inhalte – etwa kindepornografische Darstellungen – zu verlinken. Allerdings ist das hier nicht der Fall, da die Liste der Bundesprüfstelle in der veröffentlichten Form selbst schon gar keine klickbaren Links enthält, sondern nur die URLs in Textform.
>
> Andererseits kann man sich natürlich nie sicher sein, ob Behörden das Ganze nicht anders bewerten und den berühmten Anfangsverdacht bejahen, welcher dann erst mal das komplette Programm (Hausdurchsuchung etc.) in Gang setzt. So liefe es ja nicht zum ersten Mal.
>
> Etwas Vorsicht ist also angebracht. Eine inhaltliche Auseinandersetzung mit der Liste, die ja zu Recht viele Fragen aufwirft, ist ja auch ohne Verlinkung möglich.

0

by Andre Meister at July 09, 2014 12:39 PM

Neues Snowden-Dokument ausgewertet: NSA und FBI überwachen gezielt US-amerikanische Muslime

Die NSA und das FBI haben prominente muslimische US-Amerikaner heimlich überwacht. Unter den Betroffenen befinden sich Anwälte, Aktivisten und Wissenschaftler, die allesamt US-Staatsbürger sind oder eine dauerhafte Aufenthaltsgenehmigung haben. Das geht aus Dokumenten des NSA-Whistleblowers Edward Snowden hervor, die Glenn Greenwald und Murtaza Hussain auf The Intercept veröffentlicht haben.

	A	B	C	D	E	F	G	H	I
1	Email Account	Created	Case Notation	Responsible Agency	Collection Status	Expire Date	Foreign Power	Nationality	Target
2	[redacted]	10/17/06	XX.SQF[redacted]	NSA	Terminated	2/1/08		Unknown	
3	[redacted]	10/17/06	XX.SQF[redacted]	NSA	Terminated	2/1/08		Unknown	
4	[redacted]	10/30/06	XX.SQF[redacted]	NSA	Terminated	2/1/08		Unknown	
5	[redacted]	11/1/06	XX.SQF[redacted]	CIA	Terminated	2/1/08		US Person	[redacted]
6	[redacted]	11/2/06	XX.SQF[redacted]	CIA	Terminated	2/1/08		Unknown	
7	[redacted]	11/3/06	XX.SQF[redacted]	CIA	Terminated	2/1/08		Non-US Person	
8	[redacted]@cair.com*	11/9/06	XX.SQF066476	FBI	Terminated	2/1/08		US Person	
9	[redacted]	5/29/07	XX.SQF[redacted]	NSA	Terminated	2/1/08		Unknown	
10	[redacted]	8/17/07	XX.SQF[redacted]	FBI	Terminated	2/1/08		US Person	[redacted]
11	[redacted]	10/12/07	XX.SQF[redacted]	CIA	Terminated	2/1/08		Non-US Person	
12	[redacted]	10/16/07	XX.SQF[redacted]	CIA	Terminated	2/1/08		Non-US Person	
13	[redacted]	10/16/06	XX.SQF[redacted]	NSA	Terminated	2/7/08		Unknown	
14	[redacted]	10/20/06	XX.SQF[redacted]	NSA	Terminated	2/7/08		Unknown	
15	[redacted]	10/20/06	XX.SQF[redacted]	NSA	Terminated	2/7/08		Unknown	
16	[redacted]	10/20/06	XX.SQF[redacted]	NSA	Terminated	2/7/08		Non-US Person	
17	[redacted]	10/20/06	XX.SQF[redacted]	NSA	Terminated	2/7/08		Non-US Person	[redacted]
18	[redacted]	10/30/06	XX.SQF[redacted]	NSA	Terminated	2/7/08		Unknown	
19	[redacted]	10/30/06	XX.SQF[redacted]	NSA	Terminated	2/7/08		Unknown	
20	[redacted]	10/30/06	XX.SQF[redacted]	NSA	Terminated	2/7/08		Non-US Person	
21	[redacted]	10/16/07	XX.SQF[redacted]	NSA	Terminated	2/7/08		Non-US Person	
22	[redacted]	10/18/07	XX.SQF[redacted]	NSA	Terminated	2/7/08		Non-US Person	
23	[redacted]	12/11/07	XX.SQF[redacted]	FBI	Terminated	2/7/08		US Person	
24	[redacted]	12/11/07	XX.SQF[redacted]	FBI	Terminated	2/7/08		US Person	
25	[redacted]	12/11/07	XX.SQF[redacted]	FBI	Terminated	2/7/08		US Person	
26	[redacted]	12/11/07	XX.SQF[redacted]	FBI	Terminated	2/7/08		US Person	
27	[redacted]	3/27/06	XX.SQF[redacted]	CIA	Terminated	2/8/08		Unknown	
28	[redacted]@yahoo.com*	4/17/06	XX.SQF065444	FBI	Terminated	2/8/08		Unknown	
29	[redacted]	10/20/06	XX.SQF[redacted]		Terminated	2/8/08		Non-US Person	
30	[redacted]@aol.com*	5/2/07	XX.SQF075597	FBI	Terminated	2/8/08		US Person	
31	[redacted]	10/19/07	XX.SQF[redacted]	NSA	Terminated	2/8/08		Non-US Person	
32	[redacted]	10/19/07	XX.SQF[redacted]	CIA	Terminated	2/8/08		Non-US Person	
33	[redacted]	10/19/07	XX.SQF[redacted]	NSA	Terminated	2/8/08		Non-US Person	

Ein Auszug aus der Tabelle, auf die sich Greenwald und Hussein beziehen. Die markierten Einträge sind die Email-Adressen von Nihad Awad (cair.com) und Faisal Gill (Yahoo! und AOL).

Auf der Liste finden sich unter anderem die Namen bzw. Email-Adressen folgender Personen, die in Deutschland zwar weitestgehend unbekannt, aber in den USA durchaus prominent sind:

- Faisal Gill, langjähriger Republikaner, der unter George W. Bush im Department für Homeland Security arbeitete und währenddessen über eine “top-secret security clearance” verfügte
- Asim Ghafoor, Anwalt der Klienten in Fällen mit Terrorismusbezug vertrat
- Hooshang Amirahmadi, iranisch-amerikanischer Professor für Internationale Beziehungen
- Agha Saeed, ehemaliger Professor für Politikwissenschaft, der sich für muslimische Bürgerrechte und palästinensische Rechte engagiert
- Nihad Awad, Direktor des Council on American-Islamic Relations (CAIR), der größten muslimischen Bürgerrechtsorganisation in den USA

Diese fünf Köpfe hat The Intercept über die auf der Liste angegebenen Email-Adressen identifiziert und ausführlich in seinem Artikel gefeatured, zu dreien gibt es auch Video-Interviews auf Vimeo. Durch sie bekommt die Inlandsüberwachung in den USA nun ein bzw. mehrere konkrete Gesichter. In vielen weiteren Fällen sei es aber nicht möglich gewesen die Betroffenen zweifelsfrei zu bestimmen.

Die Begründungen, warum diese und andere US-Bürger überwacht wurden sind geheim, somit ist auch der genaue Umfang der Überwachung nicht bekannt. Greenwald und Hussain berichten aber, dass die meisten Menschen auf der Liste einen muslimischen Hintergrund haben. Als verantwortliche Behörde für die Überwachungsmaßnahmen ist das FBI angegeben, das beim Thema Rasterfahndung und Beobachtung von US-Muslimen über eine höchst fragwürdige Vorgeschichte verfügt.

In der Tabelle finden sich laut Greenwald und Hussain 202 Email-Adressen die US-Bürgern zugeordnet sind, 1.782 gehören zu “non-U.S. persons”, und bei 5501 weiteren ist keine Nationalität angegeben. Insgesamt sind es 7.485 Email-Adressen die zwischen 2002 und 2008 überwacht wurden. Seitdem habe sich keines der Überwachungsopfer etwas zu Schulden kommen lassen, weder terroristisch noch anderweitig.

> “Ich weiß einfach nicht warum”

sagt Faisal Gill in seinem Video-Interview und beteuert ein “guter Bürger” zu sein. Er habe in der Navy gedient, für die Regierung gearbeitet und sich gesellschaftlich engagiert. All das mache ihn zu einem Patrioten. Seine AOL und Yahoo Email-Accounts wurden überwacht, als er Kandidat für die Wahl zum Virginia House of Delegates (vergleichbar mit einem Landtag) war.

Die Genehmigung für diese Inlandsüberwachung von US-Bürgern erteilt normalerweise der, streng geheime, Foreign Intelligence

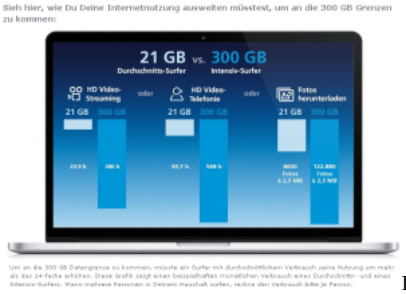
Surveillance Court (FISC). Für eine Erlaubnis muss dieses Gericht überzeugt sein, dass ein amerikanisches Überwachungsziel als Agenten einer internationalen terroristischen Organisation oder einer anderen ausländischen Macht agiert und dass es sich an Spionage, Sabotage oder Terrorismus beteiligt oder beteiligen könnte. Eine Genehmigung des FISC für die Überwachung von Inländern muss für gewöhnlich alle 90 Tage erneuert werden, ob in den konkreten Fällen auf der Liste eine Genehmigung vorlag, geht daraus nicht hervor. Die Entscheidungen des Geheimgerichts sind aber stets extrem einseitig: in 35 Jahren wurden 35.434 Überwachungsanfragen genehmigt, nur 12 wurden abgelehnt.

Um 15.00 Uhr mitteleuropäischer Zeit soll es eine Reddit AMA-Session mit den Autoren geben (hier). Die Veröffentlichung des Artikels war vor gut einer Woche kurzfristig verschoben worden, weil die US-Regierung Einsprüche erhoben hatte.

0

by Kilian Vieth at July 09, 2014 12:03 PM

Der O2-Vorteil – Jetzt auch mit Flatrate-Drossel



Das Telekommunikationsunternehmen O2 bietet seinen Kunden jetzt auch eine Flatrate mit Drossel an. Im Gegensatz zur Deutschen Telekom verbindet man dies (noch nicht) mit einer Verletzung der Netzneutralität. Kommuniziert wird die Drosselung der Flatrate als "Fair-Use-Vorteil". Warum auch immer, das geht jetzt etwas nach hinten los. Immerhin spricht man immer noch von einer Flatrate und das ist Verbraucher-Täuschung: "Mit dem Fair-Use-Vorteil ermöglichen wir Flatrate-Surfen für alle."

Das Procedere ist etwas kompliziert: Die Drosselung soll erst auftreten, wenn mehrere Monate hintereinander mehr als 300 GB pro Monat erreicht worden sind. Und dann soll man mehr zahlen können, um quasi weiterhin eine Flatrate nicht nur auf Papier und im Vertragsnamen sondern auch in der Realität zu haben. Lustig ist übrigens das Werbebild, womit die Drosselung kommuniziert wird: Wie schafft es die Marketingabteilung, in drei Balken unterschiedliche Längen für 21 GB zu bekommen?

Die Deutsche Telekom machte sich im vergangenen Jahr einen Namen als Drosselkom als sie ankündigte, zukünftig ab 75 GB bei einer 16 MB/s Flatrate auf 90er-Geschwindigkeit zu drosseln, aber eigene und Partnerangebot weiterhin bei voller Geschwindigkeit durchlassen zu wollen. Das ist eindeutig eine angekündigte Verletzung der Netzneutralität und die Ankündigung eines Zweiklassen-Netzes durch Überholspuren für zahlungskräftige Partner (bzw. eine Bevorteilung der eigenen Produkte). O2 hat das zumindest nicht angekündigt.

0

by Markus Beckedahl at July 09, 2014 10:08 AM

Wir haben eine Drohne und eine Frage an Experten

Wir besitzen jetzt eine Phantom 2 – Drohne in unserer Redaktion und haben uns dazu eine Go Pro 3 gekauft. Nun fehlt nur noch das passende Zwischenstück, in der Fachsprache Gimbal genannt, um die Kamera unter der Drohne zu befestigen und damit rumspielen zu können.

Nun ist die offizielle (und auch sonst) Empfehlung das Gimbal DJI Zenmuse H3-3D. Kostet aber rund 400 Euro und damit fast soviel wie die Drohne (und mehr als die Kamera). Es gibt eine Vielzahl an günstigen Alternativen, aber in der Regel haben diese keine oder nur eine Bewertung auf Amazon und das hält uns von einem Kauf ab. Eine günstigere Alternative mit einigen guten Bewertungen ist das "JMT 1 Set Upgrade Whole Sealing Brushless Gimbal Camera Mount W/ Motor Controller". (Kostet um die 130 Euro).

Was würdet Ihr uns empfehlen? Lieber mehr ausgeben oder Geld sparen, weil günstige ALternative dasselbe tut?

0

by Markus Beckedahl at July 09, 2014 09:52 AM

Neuer Doppelagent der USA enttarnt. Fall noch ernster. Aber keine Panik, das sind die Guten!

Es scheint ein zweiter Doppelagent bei einem deutschen Geheimdienst ("im militärischen Bereich") aufgeflogen zu sein, dessen Fall "ernster sein soll als der gerade aufgeflogene BND-Agent. Das berichtet der Rechercheverbund aus NDR, WDR und "Süddeutscher Zeitung": Spionageaffäre weitet sich aus – Zweiter Fall.

Gerade laufen Hausdurchsuchungen in Berlin, mehr Infos gibt es noch nicht.

Aber keine Panik, das ist vollkommen normal und gehört dazu. Diesen Eindruck vermittelte heute morgen Norbert Röttgen (CDU), Vorsitzender des Auswärtigen Ausschusses im Bundestag, im Deutschlandfunk-Interview.

> Auch wir Deutschen müssen vielleicht zur Kenntnis nehmen, dass es ein anderes Verständnis der Geheimdienste in den USA gibt. Das heißt, wir müssen da selber realistisch werden. Aber wir dürfen übrigens auch nicht den Fehler machen, jetzt die Dummheiten der USA auf dem Gebiet der Geheimdienste zum Maßstab zu nehmen generell für das deutsch-amerikanische Verhältnis. Das wäre sicherlich auch ein Fehler, den wir nicht machen dürfen.

Wir müssen einfach mal reden (und uns vielleicht an die Hand nehmen):

> Aber auf der anderen Seite gibt es dieses Verständnis in einer Geheimdienstbürokratie, die insbesondere nach dem Anschlag vom 11. September und dem Trauma, das dieser Anschlag ausgelöst hat – das Trauma dauert bis auf den heutigen Tag an, es prägt die Gesellschaft in den USA -, ein anderes Verständnis, das darin besteht, wir sammeln auch alles mal, was es gibt an Informationen mit den enormen Mitteln, mit dem wahnsinnig vielen Geld, das zur Verfügung steht. Darum, glaube ich, ist auch vielleicht so etwas eingetreten wie ein Kontrollverlust einer riesigen Geheimdienstbürokratie. Meine Vermutung ist eher, dass diese Dummheiten nicht auf irgendeiner politischen Ebene stattfinden, sondern im Rahmen einer sich verselbständigenden großen Geheimdienstbürokratie. Auch darüber muss geredet werden.

Es wird sich übrigens nichts ändern, aber wir können ja mal reden, dass das nicht so toll ist:

> Also die USA sind traumatisiert durch die Erlebnisse vom 11. September, sie haben eine enorme Geheimdienstbürokratie entwickelt mit enormen technologischen Möglichkeiten, enorm viel Geld. Ich rechne nicht mit einer Veränderung, sondern wir müssen darüber reden, ihnen den Schaden vor Augen führen, den wir uns außenpolitisch beide nicht leisten können.

Apropos, bevor das wieder untergeht: Was ist eigentlich mit der anlasslosen Massenüberwachung unserer Kommunikation durch US-Geheimdienste und ihrer Partner? Was machen wir mit diesen kriminell agierenden Geheimdiensten, die im Namen der Sicherheit nur massive Unsicherheit schaffen und unsere IT-Infrastrukturen kaputt machen?

0

by Markus Beckedahl at July 09, 2014 09:41 AM

July 08, 2014

CCC Dresden

Workshop De-Mail

Datum
Mittwoch, 9. Juli 2014 um 20:00 Uhr
Ort
LGS Piraten, Kamenzer Str. 13/15, 01099 Dresden

Eine kurzfristige Einladung der Piraten an die anderen Fraktionen im Stadtrat und alle Interessierten:

> nach der wirklich schoenen und konstruktiven Veranstaltung heute (gemeinsames Gucken vom Vortrag von Linus Neumann von dem letzten CCC-Kongress und anschliessender Diskussion), haben wir beschlossen, am
>
> Mittwoch, 09.07.14, 20:00 Uhr, LGS
>
> einen "Spontanworkshop" zu DE-Mail zu #machen.
>
> Warum die Eile: da die Zeit draengt. Warmum so ein Workshop: weil neue Mehrheiten im SR was aendern koennen, wir aber SCHNELL positive und konstruktive und umsetzbare Ideen brauchen. Ideen, die jetzt auch real eine Chance auf konkrete und zeitnahe Umsetzung haben! Jetzt ist also mal wirklich der "Schwarm" in Dresden gefragt.
>
> Heute war und am Mittwoch wird auch Stadtrat Thorsten Schulze (Gruene) mit dabei sein. Ich werde auch versuchen, noch Vertreter anderer Fraktionen (Linke, SPD, Buerger) einzuladen (bzw. mach ich gleich mit dieser Mail im BCC).

by CCC Dresden (mail@c3d2.de) at July 08, 2014 09:27 PM

FoeBuD e.V.

„Die größte Bedrohung seit dem Bürgerkrieg“ – NSA-Whistleblower über die Geheimdienste

Vergangene Woche hat die Bundestagsfraktion der Grünen ihre vierte netzpolitische Soirée gehalten. Zeitgleich mit dem NSA-Untersuchungsausschuss. Da dieser sehr viel länger als geplant tagte, fehlten einige Gäste. Spannend war die Diskussion trotzdem.

Eigentlich waren neben William Binney auch Thomas Drake und Jesselyn Radack angekündigt. Die beiden saßen aber bis nach Mitternacht sozusagen im Untersuchungsausschuss fest. Von dieser Sitzung gab es leider keinen Videostream, dafür aber einen grimmepreisverdächtigen Liveblog der Kollegen von Netzpolitik.

Die Grünen Fraktionsvorsitzende Katrin Göring-Eckardt eröffnete den Abend, an dem dann auch Jan-Philipp Albrecht und Georg Mascolo als Moderator eingesprungen waren. Constanze Kurz vom Chaos Computer Club saß ebenfalls – neben Binney planmäßig – auf dem Podium.

Göring-Eckardt erinnerte an ihre eigene Ostvergangenheit und die von Angela Merkel. „Das Schweigen der Kanzlerin steht einer Demokratie 25 Jahre nach dem Fall der Mauer nicht an“, so Göring-Eckardt wörtlich. Und das Schweigen wurde nur umso lauter, als einen Tag später auch noch die Spionagevorwürfe innerhalb des BND bekannt wurden...

William „Bill“ Binney sprach gewissermaßen als Insider. Lange vor Edward Snowden wurde er zum Whistleblower, nachdem er als technischer Leiter die Überwachungsprogramme der NSA mit aufgebaut hatte. Schon vor dem 11. September 2001 sei die NSA seiner Meinung nach „dysfunctional“, also funktionsgestört. Ob es eine Abhilfe sein könnte, wie Binney vorschlug, sich auf die fokussierte Überwachung Einzelner zu konzentrieren, oder ob es nicht vielmehr im Wesen der Geheimdienste liegt, alles wissen zu wollen, über alle – für diese Frage ist der ehemalige NSA-Mitarbeiter wohl die falsche Adresse.

Wir stehen an einem Wendepunkt

Sehr viel konsequenter war Constanze Kurz in ihren Statements. Leider sei es immer so, dass die Aufregung verpufft und so gut wie keine Änderungen nach sich zögen. Die Snowdenenthüllungen, die zum ersten Mal Beweise lieferten, müssten jetzt ein „Wendepunkt“ sein, sonst wäre alles Vergebens.

Auch Jan-Philip Albrecht hoffte, dass sich wirklich etwas im Umgang der Staaten mit ihren Geheimdiensten änderte. Und nicht noch mehr Zeit verloren ginge, wie nach dem Echelon-Skandal schon 15 Jahre verloren wurden. Vielmehr müssten jetzt Strafverfahren angestrengt werden, die Gesetze seien da, der Gesetzesbruch offenkundig. Lediglich die Regierungen seien ohnmächtig. Auch könnte man die Safe Harbor Entscheidung kündigen.

Ganz auf der praktischen Ebene, so Jan-Philip Albrecht, müsse offene Software gefördert werden. Es sei fast schon kriminell angesichts der aktuellen Situation, Microsoft Produkte in Behörden einzusetzen, da könne der Datenschutz überhaupt nicht überprüft werden.

Binney, der zuvor dem Untersuchungsausschuss sechs Stunden lang Rede und Antwort stand, setzte sich für die Idee einer echten Kontrolle ein, für die er technisches Know-How forderte. Weshalb also nicht die Geheimdienste von Hackern kontrollieren lassen, fragte er und erntete prompte Ablehnung der Hackerin Constanze Kurz. Vor Snowden, so die Sprecherin des CCC, hätte man darüber reden können. Mittlerweile seien die Geheimdienste nicht mehr kontrollierbar, sondern abzuschaffen. „Wir müssen klar und deutlich als Ziel formulieren, das nicht mehr zu finanzieren,“ so Kurz.

Das vollständige Video der Veranstaltung gibt es auf Grün-Digital.

(Bild: Dennis Romberg, cc-by)

Tags:
NSA
Geheimdienste
Späh-Affäre
Geheimdienst-Affäre
jan philipp albrecht
bill binney
NSA-Affäre

by Dennis Romberg at July 08, 2014 07:04 PM

Netzpolitik.org

Zukunftsmodell „intelligente Stadt“: Wir brauchen mehr intelligente Dörfer

Evgeny Morozov schreibt in der FAZ über das Zukunftsmodell „intelligente Stadt“: Wir brauchen mehr intelligente Dörfer.

> Aber wie übersetzt man diese humanistische Haltung in konkrete Technologien? Selbst die Kritiker helfen uns da kaum weiter. Vielleicht könnte man mit der Frage anfangen, wie das Gegenteil der von IT-Konzernen gesteuerten „intelligenten Stadt“ aussieht. Wodurch zeichnet sich ihr ideologischer Antipode aus? Ist es die „dumme Stadt“? Heutzutage, wo Mülleimer mit Sensoren und Straßenlaternen mit hochentwickelten Kameras ausgestattet sind, ist die Sehnsucht nach einer analogen Stadt absolut verständlich, zumal nach dem NSA-Skandal. Doch diese Nostalgie ist historisch wenig tragfähig – Städte waren schon immer Versuchsfelder für revolutionäre Neuerungen, ob Kanalisation, Impfstoffe oder Untergrundbahn. Eine technikfreie Stadt kann nicht als Vorbild dienen.

0

by Markus Beckedahl at July 08, 2014 06:42 PM

The Ex-Google Hacker Taking on the World’s Spy Agencies

Wired hat ein schönes Portrait über Morgan Marquis-Boire (@headhntr), der jetzt von Google zu Glenn Greenwalds First Look Media gewechselt ist und dort für die Sicherheit zuständig ist: The Ex-Google Hacker Taking on the World’s Spy Agencies.

> Beyond protecting Snowden’s favorite journalists, Marquis-Boire sees his decision to leave Google for First Look as a chance to focus full-time on the problem of protecting reporters and activists as a whole, groups he sees as some of the most sensitive targets for governments globally. “I look at the risk posed to individuals in the real world,” says Marquis-Boire, an imposing, often black-clad New Zealander with earrings, dreadlocks, and a taste for death metal. “In human rights and journalism, the consequences of communications being compromised are imprisonment, physical violence, and even death. These types of users need security assistance in a very real sense.”

Auf der vergangenen re:publica’14 sprach Morgan Marquis-Boire über Staatstrojaner und “Fear and Loathing on the Internet“:

0

by Markus Beckedahl at July 08, 2014 03:09 PM

Heute, 8. Juli, 20h, Berlin: Datengarten zu Indischen Staats-Datenbanken

Im Chaos Computer Club Berlin findet heute Abend ein Votragsabend – "Datengarten" – statt, welcher sich mit den Bestrebungen der indischen Regierung auseinandersetzt eine umfangreiche Datenbank der Bevölkerung inkl. biometrischer Daten anzulegen. Der Referent Sumandro Chattapadhyay forscht zum Themenbereich Informationspolitik in Indien im Centre for the Study of Developing Societies in Dehli.

Der Vortrag beginnt um 20h und findet in englischer Sprache statt. Aus der Ankündigung:

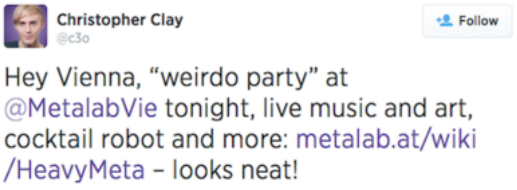
> **What kind of 'database state' is the Indian government creating?**
>
> A discussion of the Aadhaar project as a digital identity platform for governance
>
> As part of my larger academic interest in the history of electronic governance and computing by the Government of India since 1960s, I have been studying the making and activities of the Unique Identification Authority of India (UIDAI). UIDAI was instituted in 2009 to assign unique biometrics- linked identification numbers, branded as Aadhaar numbers, to all the residents of India. The growing literature about this Aadhaar project focus on various topics such as implications for citizenship, for efficiency of governmental services, for formalisation and unification of unorganised banking and welfare-accessing practices. As opposed to socio-legal critiques offered by most researchers and activists in India, I discuss the technological imagination and the materiality of the database system being designed and deployed as part of the Aadhaar project. I argue that it is crucial to develop a close understanding of the specific form of data collection, management, archiving, sharing by the Aadhaar project and the software infrastructure it is building to enable various government and commercial agencies to implement a single identity platform for tracking their interactions with citizens/consumers. [...]

0

by Matthias Mehldau at July 08, 2014 01:35 PM

Metalab

[alphabet] --c3o on Twitter



--c3o on Twitter

July 08, 2014 01:26 PM

Netzpolitik.org

Ägyptische Blogger im Gefängnis – eine emotionale Erzählung über Schmerz, Liebe und Hoffnung

Dieser Beitrag wurde ursprünglich auf Arabisch von Mona Seif geschrieben. Ihr Bruder Alaa Abd El Fattah sitzt momentan eine 15-jährige Haftstrafe wegen Teilnahme an einer Demonstration ab. Ihre Schwester Sanaa Seif ist auch im Gefängnis, ihr steht ein Gerichtsverfahren bevor, weil sie an einer Demonstration gegen ein umstrittenes ägyptisches Gesetz teilgenommen hat, das Demonstrationen verbietet. Wir haben die englische Version ihres Blogposts von Amira Al Hussaini, der vom Schmerz, der Liebe und der Hoffnung ihrer Familie erzählt, hier auf Deutsch übersetzt.

Als Kind war der Tod die größte Angst, die ich hatte.

Ich hatte viele Alpträume. Die Vorstellung meines Todes jagte mich, und ich weinte mir die Augen aus, während ich allein im Bett lag. Meine Mutter sagte mir, dass es meiner Tante genauso gegangen war, als sie noch ein Kind war. Meine Mutter hat diese Angst von mir und meiner Tante nie verstanden, aber sie war immer diejenige, die uns half damit umzugehen. Als ich mit meiner Tante darüber sprach, erzählte sie mir, dass sich ihre Angst vor dem Tod durch die Geburt ihrer Kinder verändert hat. Ich habe ihre Worte nicht verstanden, bis

ich meine Gefühle für Sanaa begriff. Sie ist meine jüngste Schwester, größer als ich und die wunderbarste Person in meinem Leben.

Als meine Mutter mit Sanaa schwanger war, fragte sie mich, ob ich lieber eine Schwester oder einen Bruder möchte. Es war eine schwierige Entscheidung für eine Achtjährige, vor allem, weil ich zwischen der Vorstellung, eine Schwester zu haben und damit ein Stockbett zu bekommen, in dem ich oben schlafen könnte, und der Vorstellung einen jüngeren Bruder zu haben, der wiederum meinen älteren Bruder würde ärgern können, hin und her gerissen war. Nach einer langen Zeit der Verwirrung, beschloss ich, dass ich Sanaa wollte und nicht Yousif, oder viel mehr, dass ich lieber ein Stockbett wollte und dafür einen anderen Wegen suchen würde um Alaa zu ärgern.

Ich erinnere mich an den Tag, als sie geboren wurde.

Unsere Verwandte Azza weckte Alaa und mich auf, um uns für die Schule fertig zu machen. Wir wussten, dass unsere Mutter um Mitternacht für die Geburt ins Krankenhaus gefahren war. Wir gingen wie in Trance zur Schule, sprangen durch den Schulhof, und Alaa rief allen zu: „Meine Schwester ist da“.

Nach der Schule nahmen wir den Bus und rannten von der Bushaltestelle bis nach Hause um die Wette. Wir betraten das Zimmer meiner Mutter, die ruhig lächelnd ein kleines Geschöpf im Arm hielt. Wir beugten uns über sie, um Sanaa genauer betrachten zu können. Sie antwortete mit einem schwachen: „Aaaaaa“. Alaa lachte und sagte „Armes Ding! Sie kann nicht mal schreien“, was Sanaa dazu veranlasste in einer Art und Weise zu kreischen, die uns kurz einen Schritt zurücktreten ließ, bevor wir vor Lachen zusammenbrachen.

So ist Sanaa. Sie vermittelt dir den Eindruck, dass sie zu schwach ist und sich nicht durchsetzen kann. Und plötzlich überrascht sie dich mit etwas, darunter auch Dinge, die du selbst nie tun könntest. Ich erinnere mich an den Tag, als wir nach dem Kabinettsvorfall zum Untersuchungsrichter fuhren, um nach unserer Verhaftung und Belästigung dort unsere Aussagen zu machen. Für alle, die uns kannten, war klar, dass ich diejenige sein würde, die sich an Aussagen, Informationen und Details erinnert, und die sich auf alles konzentrieren würde, während Sanaa diejenige war, die in ihrer eigenen Fantasiewelt lebte, und Namen und Details vergessen würde. An diesem Tag hat sie mich wieder überrascht. Ich begann zu erzählen, was passiert war – Gefühle, Namen und Beschreibungen der Menschen, die vor Ort waren. Mir wurde dann erklärt, dass das alles irrelevant sei und dass ich Beschreibungen präsentieren soll, die helfen würden, die Leute zu finden, die uns belästigt hatten. Ich verwende immer automatisch einen der Überlebenstricks, die das tägliche Leben mit Belästigungen auf der Straßen mit sich bringt: ich versuche die Gesichter und Merkmale all dieser Menschen, vor denen ich Angst habe und die mich bedrohen, zu verwischen.

Sanaa hingegen, meine Schwester, die alle Brücken in Kairo als Tharwat Brücke bezeichnet (weil es der einzige Brückenname ist, den sie kennt), setzte sich vor den Richter und gab ihm eine detaillierte Beschreibung all jener, die uns angegriffen hatten und aller Personen die gemeinsam mit uns verhaftet worden waren. Sie konnte ihre Größe, ihrer Hautfarbe und die Anzahl der Sterne und Abzeichen auf ihren Schultern beschreiben. Und sie identifizierte drei der Offiziere, die uns angegriffen hatten, auf Basis von Zeitungsberichten.

Ich erinnere mich, wie ich dann mit ihr scherzte: „Wer bist du? Gib mir meine Schwester Sanaa zurück!“ Ich erinnere mich auch, dass mir an diesem Tag klar wurde, wie wichtig Sanaa in lebensverändernden Momenten war, dass sie anders war, und dass ihre Fähigkeit, sich zu konzentrieren und Entscheidungen zu treffen, die aller anderen Menschen, die ich kannte, übertraf.

Seit ein paar Tagen habe ich nun diesen Schmerz in mir unterdrückt, den ich nicht bewältigen kann. Dieser Schmerz hängt damit zusammen, dass alle Versuche, die eine ältere Schwester unternehmen kann, um ihre jüngere Schwester zu beschützen, gescheitert sind. Es ist ein Schmerz über diese drei Minuten, die ich sie an der Polizeistation sah, als wir von einer Tür und Stacheldraht getrennt waren, und ich sie nicht umarmen konnte. Und darüber, dass wir unsere ganze Unterhaltung gehetzt und mit lauter Stimme führen mussten, als Versuch, sie und die anderen Häftlinge zu beruhigen. Sie sah das Ganze wahrscheinlich als eine Menge Gerede, voller Angst, und voller Forderungen und Anweisungen von mir.

Im Moment ist das Leben so hart zu uns, dass man es nicht einmal schafft, den Schmerz zu begreifen, die Trauer auszudrücken oder über die Liebe zu seinen inhaftierten Geschwistern zu sprechen. Als ich heute Sanaa besuchte, brauchte es nur einen kleinen Brief und ein paar Worte von ihr, um mich von all dem Schmerz zu befreien. Wieder hat sie mich überrascht, denn trotz der Entfernung und der Gefängnismauern zwischen uns, war nur sie in der Lage, meinen Schmerz zu verstehen.

Im Dezember letzten Jahres schrieb ich, nach einem Besuch bei Alaa im Gefängnis:

„Eure Gefängnisse schrecken uns nicht ab.
Wenn uns eure Ungerechtigkeit verletzt, wird der Tag kommen, an dem wir uns an all die schönen Dinge von denen wir träumen, erinnern, die uns darauf beharren lassen, unsere Alpträume zu besiegen.
Und wir werden uns an das Lachen all jener erinnern, von denen wir getrennt wurden.
Wir haben eine Geheimwaffe. Wir haben Sanaa.
Wahrlich, mit all euren Panzern und Gefängnissen, und gepanzerten Fahrzeugen und Leichenhallen … wir sind stärker als ihr.“

Es ist zwar richtig, dass sie Gefängnisse, gepanzerte Fahrzeuge, Patronen, Gerichte und Polizeistationen haben. Und, dass sie in der Lage sind, uns voneinander zu trennen, wie mit Alaa im Tora-Gefängnis und Sanaa im Qanater-Gefängnis, wodurch wir Besuchsgenehmigung für Alaas Gefängnis am Zenhum-Gericht und für Sanaas Gefängnis am Al Abbasiya-Gericht beantragen müssen. Aber wir haben noch eine Geheimwaffe: Sanaa und die überquellende Fähigkeit zu lieben, die alle Gefängniswände überragt.

0

by Kilian Vieth at July 08, 2014 01:21 PM

Metalab

[alphabet] --nightlibrarian on Twitter

--nightlibrarian on Twitter

July 08, 2014 01:13 PM

Netzpolitik.org

"Smart Target Enhancement Program" erklärt den "Five Eyes", wo nicht spioniert werden darf

Die britische Bürgerrechtsorganisation hat ein pdf republiziert, aus dem hervorgeht in welchen Ländern US-Geheimdienste nicht aktiv werden dürfen. Das als geheim eingestufte Dokument trägt den Titel "Smart Target Enhancement Program" (STEP) und widmet sich "Non-targetable 2nd Party Countries, Territories & Individuals". Es soll offensichtlich die Zusammenarbeit jener Staaten regeln, die in den "Five Eyes" zusammengeschlossen sind (Kanada, Großbritannien, Neuseeland, USA, Australien).

Nicht nur auf dem Festland dieser Länder darf laut dem "Smart Target Enhancement Program" nicht spioniert werden: Aufgelistet sind auch ehemalige Kolonien, die jetzt zu den "Five Eyes" gehören. So darf zum Beispiel auch auf den Falkland Inseln oder Gibraltar nicht abgehört werden.

Hinweise gibt es auch zu Top Level Domains, die von der digitalen Spionage ausgenommen bleiben sollen. Hierzu gehören die Inseln Saint Helena oder die Nördlichen Marianen, aber auch Guernsey, Jersey und die Isle of Man.

Im Dokument findet sich auch eine kleine Tabelle zu Überwachungsbefugnissen und benötigten Beschlüssen. Unterteilt wird in vier Kategorien: Eigene Staatsangehörige im eigenen Land, eigene Staatsangehörige anderswo, ausländische Staatsangehörige im eigenen Land, ausländische Staatsangehörige anderswo.

Die letzte Kategorie bietet bekanntlich am wenigsten Schutz: Die Überwachung sei "rechtmäßig ohne besondere Genehmigung" ("Lawful without specific authorization"). Im Falle der NSA heißt es zur Überwachung ausländischer Staatsangehöriger in den USA, dies erfordere immer eine FISA-Anordnung und sei "sehr komplex".

Targeting Authorization Requirements

Country	National in ...*	National overseas	Foreign national in ...	Foreign national overseas
Australia (DSD)	Warrant and Ministerial Authorization	Ministerial authorization	International comms OK; warrant if domestic	Lawful without specific authorization
Canada (CSEC)	Cannot target Canadians	Cannot target Canadians	Considered to be Canadian - CSEC cannot target	Lawful without specific authorization, but ministerial authorization needed if CSEC intercepts private communications of Canadians in relation to the activity or class of activities specified in the authorization
New Zealand (GCSB)	Cannot target unless Agent of a Foreign Power; if so, international comms OK; warrant required if domestic	Cannot do it unless Agent of a Foreign Power	International comms ok; Warrant if domestic	Lawful without specific authorization
UK (GCHQ)	Warrant	STA	Warrant	Lawful without specific authorization
USA (NSA)	FISA warrant and probable agent of a foreign power	FISA warrant and agent of a foreign power	Generally a FISA warrant, however rules depend on situation - very complex	Lawful without specific authorization

Unbekannt ist das pdf übrigens nicht: Es erschien bereits auf der Webseite Canleaks und soll dort im Januar 2007 hochgeladen worden sein.

0

by Matthias Monroy at July 08, 2014 12:49 PM

Liste indizierter Webseiten geleakt: Bundesprüfstelle bestätigt Netz-Sperren-Kritik wie Overblocking

Bundesprüfstelle für jugendgefährdende Medien

Die geheime Liste an in Deutschland indizierten Webseiten sperrt viel mehr, als ihr Auftrag. Das ist

jetzt überprüfbar, da eine anonyme Hackerin die Liste an über 3.000 URLs reverse-engineered und veröffentlicht hat. Fast die Hälfte aller der als jugendgefährdend eingestuften Webseiten existiert gar nicht mehr.

Über die Bundesprüfstelle für jugendgefährdende Medien (BPjM) haben wir hier bereits öfters berichtet. Wikipedia sagt:

> Ihre Zuständigkeit liegt in der Prüfung und Aufnahme von Medien in die Liste jugendgefährdender Medien („Indizierung“). Sie dient dem medialen Jugendschutz.

Zum Inhalt von diesem Index weiß die Wikipedia:

> Bei so genannten Telemedien unterbleibt eine Veröffentlichung, um einen Werbeeffekt zu vermeiden.
> […]
> Bezüglich der Liste der nicht veröffentlichten Telemedien wird diese gemäß § 24 Abs. 5 JuSchG anerkannten Einrichtungen der Selbstkontrolle zum Zweck der Aufnahme in nutzerautonome Filterprogramme in verschlüsselter Form zur Verfügung gestellt. Dies betrifft etwa die Selbstkontrolle der Betreiber von Suchmaschinen.

Nun ist das mit dieser Verschlüsselung immer so eine Sache. Ein findiger, anonymer Nerd hat jetzt die Hashwerte der veröffentlichten Liste zurückgerechnet und als BPjM-Leak veröffentlicht **[Update: Uns wurde wegen des Links mit Klage gedroht. Wir haben den Link rausgenommen und unsere Position in einem extra Beitrag erklärt.]**.

Die Liste an zensierten “Telemedien” (URLs von Webseiten) geht OpenPGP-verschlüsselt an Suchmaschinen, oder als kryptografische Hashwerte an Router-Hersteller wie AVM FRITZ!Box. Von jedem Router kann man diese monatlich automatisch aktualisierte Liste herunterkopieren und analysieren. Das Zurückrechnen der Hashes zu URLs vereinfacht sich merklich, wenn man statt Brute-Force-Methode bereits andere veröffentliche Sperrlisten und Listen von Webseiten verwendet. So war der (oder die) Hackerin in der Lage, 3.280 MD5-Hashes und 2.889 SHA1 Hashes zu errechnen.

Damit ist das allererste Mal ein umfassender öffentlicher Einblick möglich, welche Webseiten der deutsche Staat zu Jugendschutzzwecken zensiert. Und das Ergebnis überrascht wenig:

> Die meisten Einträge der liste können als eine der folgenden Kategorien eingestuft werden: normale Pornografie, Tierpornografie, Kinder-/Jugendpornografie, Suizid, Nazis oder Anorexie. Auf nur etwa 50-60% der Domains auf der Liste sind die fragwürdigen Inhalten noch zugänglich: Über 10% der Domains sind nicht registriert, weitere 10% sind geparkte Domains, und etwa 20% stellen überhaupt keine Inhalte zur Verfügung (entweder kein DNS-A-Eintrag, kein Webserver auf Port 80 oder eine Umleitung zu einer anderen Domain).

Warum das so ist, steht im Gesetz: Erst nach Ablauf von 25 Jahren verliert eine Aufnahme in die Liste ihre Wirkung. Das sind nicht gerade internet-kompatible Zeiteinheiten.

Und dann sind da die bei Sperrlisten üblichen Falsch-Einträge:

- **irgend.ein.name.homo.com** – homo.com ist eine Wildcard-Seite, die bei jeder subdomain.homo.com einen (fragwürdigen) Inhalt liefert.
- **amazon.co.uk/Deep-Silver-Dead-Island-Xbox** – Ein einziges “über 18″ Spiel ist auf dem (britischen) Amazon gesperrt. Man würde entweder alle oder keine erwarten. (Mal abgesehen davon, dass Amazon zig verschiedene URLs pro Produkt hat.)
- **discogs.com/sell/list** – Laut Wikipedia ist Discogs “eine kostenlose, von Mitgliedern aufgebaute Online-Datenbank für Diskografien von Musikern und Plattenlabeln. Mit einem Alexa Rank von 1757 im Oktober 2011 zählt sie zu den meistbesuchten Websites der Welt.” Es wird also eine ganze Bibliothek gesperrt, weil vielleicht ein paar Bücher jugendgefährdend sein können? Klassischer Fall von Overblocking.
- **bible.org/seriespage/weisheit-und-kindererziehung-teil-iii** – Nun, vielleicht verdient der Artikel “Warum die Rute gerecht ist” nicht nur eine Sperre, sondern Strafverfolgung?
- Vertipper wie **bilola**, **hot-soccer-moms-info** und **www-gangbang-squad.com**.

Und natürlich viele, viele nicht mehr existierende Seiten.

Alles in allem scheint sich mal wieder zu bestätigen, was auch in bisherigen Analysen geleakter Sperrlisten festgestellt wurde (wie beispielsweise von Matti Nikki in Finnland und vom AK Zensur über die Listen in Dänemark und Schweden): Es ist nicht möglich, Sperrlisten geheim zu halten. Sperrlisten sind sehr fehleranfällig und zensieren mehr als ihr Auftrag. Interessierte finden immer einen Weg, sie zu umgehen. Aber die Gefahr für Meinungs- und Informationsfreiheit ist größer als ihr (vermeintlicher) Nutzen.

Das bestätigt auch Alvar Freude vom Arbeitskreis gegen Internet-Sperren und Zensur (AK Zensur) gegenüber netzpolitik.org:

> Der Leak zeigt, wie bei der Diskussion um das Zugangserschwerungsgesetz, dass solche Filterlisten nie geheim bleiben. Und dann werden sie eben zum Wegweiser für die “interessantesten” Seiten. Der Leak zeigt aber auch, dass auf solchen Listen immer wieder Webseiten landen, die dort nicht hin gehören: Die Inhalte (und Inhaber) von Webseiten können sich schnell ändern, eine 25 Jahre gültige Indizierung wird dem nicht gerecht. Die Realität ist, dass heutzutage jeder durchschnittlich intelligente 15 jährige Jugendliche so viel Pornografie finden kann, wie er nie konsumieren können wird – kein Filterprogramm oder die Indizierung durch die BPjM ändert daran etwas, das ist nur eine Beruhigungspille für eine überforderte Gesellschaft. Wenn Eltern ihren Kindern Filter installieren wollen, dann können sie das machen – eine staatlich sanktionierte Zensurliste passt aber, egal wie gut sie gemeint ist, nicht zu unserer freiheitlich-demokratischen Grundordnung.

Erst letzte Woche wurde bekannt, dass der “freiwillige” “Porno-Filter” in Großbritannien jede fünfte Webseiten sperrt.

Netzpolitik.org-Mitblogger Andreas Müller hat ebenfalls eine Sperrliste reverse-engineered: Er hat die Millionen Alexa Topsites gegen den KinderServer (proxy.kinderserver.eu:3128) getestet und festgestellt, dass 987.526 (95.93 %) Domains geblockt und nur 1.095 (0.11%) Domains erlaubt werden.

Wir haben sowohl dem Hacker/der Hackerin als auch der BPjM einige Anfragen geschickt und werden diese ergänzen, sobald die Antworten da sind.

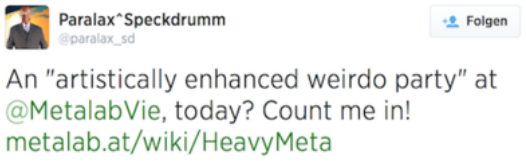
Update: Es sind auch 37 .de-Domains auf der Liste. Ist das überhaupt rechtmäßig? Oder müssen die nicht eh dem (umstrittenen) Jugendmedienschutz-Staatsvertrag genügen?

0

by Andre Meister at July 08, 2014 12:04 PM

Metalab

[alphabet] -- paralax_sd on Twitter



-- paralax_sd on Twitter

July 08, 2014 11:32 AM

Netzpolitik.org

Die Zukunft des Internets: Pew Studie identifiziert die vier größten Bedrohungen für ein freies Netz

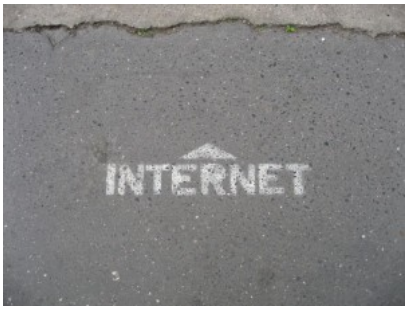


Foto: Mike Lee | flickr | CC-BY-NC 2.0

Tagesaktuelle Meldungen über Bedrohungen des Netzes sind unser Geschäft. Wir verbloggen, was wichtig ist, was jetzt passiert, was im Moment vor sich geht. Da bleibt kaum Zeit, um einmal innezuhalten und darüber zu sinnieren, wie das alles in fünf oder zehn Jahren aussieht. Welche Themen dann noch nachwirken, was vielleicht noch immer aktuell ist? Eine neue Studie des Pew Research Institutes vom 3. Juli mit dem Titel "Digital Life in 2025. Net Threats" geht dieser Frage nun nach.

Um ein Bild einer möglichen Zukunft zu zeichnen, greifen die Macher der Studie statt zu quantitativen, statistischen Methoden lieber zum 'canvassing', d.h. sie gingen auf drei unterschiedlicher Expertengruppen zu: Bekannte Internetexperten sowie Analysten aus der Tech-Industrie und schließlich über spezifische Mailing-Listen des Pew Research Institutes. Über 1400 beantworteten die Frage:

> **Accessing and sharing content online** – By 2025, will there be significant changes for the worse and hindrances to the ways in which people get and share content online compared with the way globally networked people can operate online today?

(Deutsche Übersetzung: Online-Zugang und Teilen von Inhalten: Werden bis 2025 signifikante Veränderungen zum Schlechteren oder Hindernisse für die Art und Weise, wie man online an Inhalte kommt und diese teilt, auftreten, verglichen mit der Art wie global vernetzte Menschen heute online handeln können?)

Zu dieser Ja-Nein-Frage konnten die Befragten noch eine Einschätzung der größten Bedrohungen und möglichen Gegenmaßnahmen liefern, sowohl anonym als auch namentlich.

Ganze 65% der Teilnehmer antworteten auf die Eingangfrage mit "Nein", nur 35% mit "Ja". Darin drückt sich der Glaube an ein freies Internet auch in der Zukunft aus. Für viele steht dieser Optimismus jedoch nicht für sich und ist mehr Hoffnung als definitive Überzeugung. Die Studie identifiziert vier große Bedrohungen, die den befragten Experten Sorgen bereiten:

1) Nationalstaatliche Bedenken um Sicherheit und politische Kontrolle werden zu stärkerer Zensur, Filterung, Fragmentierung und Balkanisierung des Internet führen.

Wenn Staaten wie China und Türkei Inhalte im Netz zensieren oder Zugänge blockieren, so tun sie dass unter Berufung auf nationale Sicherheit, Integrität und moralische Schutzansprüche. Häufig ist es aber vor allem politische Kontrolle, die darüber stabilisiert werden soll. Paul Saffo (Discern Analytics/Universität Stanford) sagt in der Studie: "Regierungen werden immer besser in der Blockierung von Zugängen zu unwillkommenen Webseiten.". Christopher Wilkinson, Vorstandsmitglied von EURid.eu, formulierte: "Überwachung… kühlt bestenfalls Kommunikation ab und schlimmstenfalls erleichtert sie Industriespionage, aber sie hat nicht besonders viel mit Sicherheit zu tun." Auch regionale Schutzbedenken wie wirtschaftlicher Protektionismus aber auch Datenschutzinitiativen können zu "Flaschenhälsen" werden die das freie Internet bedrohen. Dem gegenüber stehen optimistischere Sichtweisen, die argumentieren, Offenheit und Innovation würden Kontrolle übertrumpfen:

> It won't be a bloodless revolution, sadly, but it will be a revolution nonetheless. – Paul Jones, ibiblio.org

2) Im Zuge der Enthüllungen über Regierungs- und industrielle Überwachung und angesichts wahrscheinlich noch stärkerer Überwachung wird sich Vertrauen in Zukunft verflüchtigen.

Den Experten zufolge stellt die umfangreiche Massen- bis hin zur Totalüberwachung eine deutliche Bedrohung für freien Zugang und Teilen von Inhalten dar. Peter S. Vogel (Internetrecht-Experte bei Gardere Wynne Sewell) sagte dazu: "Datenschutzfragen sind die größte Bedrohung für den Zugang zu und den Austausch von Internet-Inhalten im Jahr 2014, und es gibt wenig Grund zu erwarten, dass sich das bis zum Jahr 2025 ändern wird, insbesondere angesichts der Cyber-Terror-Bedrohungen mit denen Internet-Nutzer und Unternehmen weltweit konfrontiert sind." Die Snowden-Enthüllungen würden zu einer stärkeren 'Balkanisierung', also Zersetzung/Fragmentierung des Internets führen, weil immer mehr Internetnutzer sich vor den Zugriffen der Sicherheitsbehörden schützen wollen, so Kate Crawford (Professorin und Forscherin).

3) Kommerzieller Druck, der alles von der Internet-Infrastruktur bis zum Informationsfluss beeinflusst, wird die offene Struktur des Online-Lebens gefährden.

Die zentralen Probleme an dieser Stelle sind das Netzneutralitätsprinzip, was immer häufiger untergraben wird, Kopierschutzbestimmungen und Patentgesetzgebung und die Kurzsichtigkeit von Regierungen und Unternehmen. Durch Absprachen und wettbewerbsfeindliche Praktiken werde die erneute Schaffung eines Internets der Leute verhindert, so ein anonymer Chefberater.

> Es ist sehr gut möglich, dass das Prinzip der Netzneutralität unterlaufen wird. In einer politischen Realität, wo die Positionen mit Geld gekauft werden, hängt viel davon ab, wie viel ISPs und Content-Anbieter bereit und in der Lage sind, für die Verteidigung ihre konkurrierenden Interessen zu zahlen. Leider zählen die Interessen der täglichen Nutzer sehr wenig. – PJ Rey, Doktorand

Dem gegenüber stehen hoffnungsvollere Perspektiven, denen zufolge wirtschaftliche und soziale Anreize die Bedrohung abmildern können. Es müsse nur die Marktmacht großer Unternehmen gebrochen und dem einzelnen Nutzer die Kontrolle zurückgegeben werden:

> [C]ontinuing to dismantle the 'middle men' is key. -Glenn Edens, PARC

4) Bemühungen, dem TMI-Problem (Too much Information – zu viele Informationen) zu begegnen, könnten zu Überkompensation führen und das Teilen von Inhalten vereiteln

Informationsströme könnten aufgrund von Filter-Algorithmen sehr stark eingeschränkt und manipuliert werden. Von einem offenen und freien Internet würde dann nicht mehr die Rede sein.

> Der Trend, Informationen immer weiter und einfacherer verfügbar zu machen wird sicher 2025 andauern. Die größte Herausforderung wird dann wohl das Problem sein, guten und sinnvollen Inhalt zu finden wenn man will. – Joel Halpern, Ericsson

Die Bedrohungen sind nicht neu

Wer regelmäßig unseren Blog liest, dem fällt auf, dass hier vorrangig Themen angesprochen werden, mit denen wir uns schon seit Jahren beschäftigen und auf deren Problematik wir beständig hinweisen. Sicher sind einige der Experten, die im Zuge dieser Studie befragt worden sind, nicht unbedingt unserer Meinung was beispielsweise Privatsphäre und Datenschutz angeht. Der allgemeine Trend jedoch lautet: Wenn jetzt nicht gegen Netzneutralitätsverstöße, Totalüberwachung, unpassendes Urheberrecht und marktbeherrschende Internetfirmen vorgegangen wird, mit allen zur Verfügung stehenden rechtlichen, politischen und technologischen Mitteln, dann wird es ein freies Netz bis 2025 sicher nicht (mehr) geben. Die Studie mag mit Eventualitäten herumspielen und sich auf Expertenmeinungen berufen, aber wer daraus nur Zukunftsmusik liest, der liest sie falsch: Die Bedrohungen von morgen sind unsere Aufgaben von heute!

0

by Elisabeth Pohl at July 08, 2014 11:22 AM

Universität in Athen will auf Geheiß eines Call Centers dem linken Serverprojekt Espiv den Stecker ziehen (Update: wieder da)

Der Rektor der Panteion Universität in Athen will das linke Serverprojekt Espiv vom Netz nehmen. Dies teilte das Administrationskollektiv "Cybrigade" am gestrigen Montag mit. Hintergrund ist die Beschwerde des Call-Center Unternehmens OnLine Sales. Der Chef der Firma verlangt, ein unliebsames Posting zu entfernen. Der Mann fühlt sich darin beleidigt. Das Löschen des Eintrags ist aber nicht die einzige Forderung: Espiv soll die Namen der AutorInnen nennen.

Wie bei unabhängigen Internetdiensten üblich weigert sich Cybrigade aber, irgendwelche Daten herauszugeben. Die seit sechs Jahren bestehende Gruppe macht darauf aufmerksam, dass keine IP-Adressen geloggt würden. Espiv betreibt die Domains espivblogs.net und espiv.net und sieht sich als eine Internet-Infrastruktur "gegen Kapitalismus und Hierarchie". Die Gruppe setzt sich nach Selbstauskunft für "digitale Rechte, das unberührbare Recht auf Privatsphäre, abhörfreie Kommunikation und freie Meinungsäußerung" ein.

Nun republiziert das Kollektiv das beanstandete Posting in mehreren Sprachen. Darin wird zu einer Kundgebung bei OnLine Sales aufgerufen da der Arbeitgeber sich weigere Überstunden auszuzahlen ohne dass die betreffende Angestellte das "Verkaufsziel" der Firma erreicht habe. Die Frau sei darüber hinaus verbal und körperlich angegriffen worden.

Bislang scheint es keine gerichtliche oder polizeiliche Handhabe zu geben: Das Schreiben von OnLine Sales war laut der Mitteilung von espiv eine "außergerichtliche Mitteilung" an die Universitätsverwaltung. In Griechenland haben Polizeibehörden traditionell keinen Zugang zu Universitäten. Das mag der Grund sein, weshalb neben vielen politischen Gruppen auch Serverprojekte den staatlich garantierten Schutz der Meinungsfreiheit suchen.

Auch Indymedia Athen parkt seine Serverfarm auf einem Hochschulgelände. Die linke Webseite hatte letztes Jahr mit dem gleichen Problem zu tun: Ein Hochschulrektor ließ den Stecker ziehen, angeblich auf Anordnung von Behörden. Die hatten aber jede Beteiligung bestritten. Später machte Indymedia öffentlich, dass wohl doch der Rektor der Technischen Universität hinter der Repressalie steckte.

Der Vorfall erinnert aber auch an die Auseinandersetzung der früher in den USA gehosteten Domain ucrony.net mit dem deutschen Schauspieler Til Schweiger. Schweiger hatte sich geärgert, dass auf einer Unterseite des Ucrony-Kollektivs ein Artikel über einen Anschlag gegen sein Wohnhaus erschien. In dem Posting hieß es, das "Millionenobjekt" von Schweiger sei deswegen adressiert worden, da der frisch gebackene Tatort-Kommissar kurz zuvor in der Bildzeitung sein "Afghanistan-Tagebuch" veröffentlichte (hier gespiegelt bei

Indymedia). Auch seine Wohnadresse war genannt worden.

Über seine Anwälte der Berliner Kanzlei Eisenberg und König hatte Schweiger schließlich erreicht, den mehrsprachigen Blog directactionde.ucrony.net abzuschalten. Die auf Medienrecht spezialisierten Anwälte erwirkten hierzu eine einstweilige Verfügung vom Landgericht Berlin gegen den Domain-Registrar domaindiscount24. Dieser sperrte daraufhin umgehend die komplette Top-Level-Domain. Gleichzeitig wurde auch jede Berichterstattung über die Maßnahme untersagt: Laut einer Presseerklärung des Betreiberkollektivs verbieten die Anwälte "ausdrücklich jedwede auch nur indirekte publizistische Nutzung" des rechtlichen Vorgehens Schweigers.

Ucrony.net bezeichnete sich als ein "Kollektiv von Freiwilligen", das seit 2006 Privatpersonen und nicht-kommerziellen Projekten Subdomains anbot. Jetzt nicht mehr: Alle Webseiten von Bürgerinitiativen, Fotografen und Musikern in den USA, Deutschland, Großbritannien und Frankreich sowie sämtliche Mailserver bleiben seitdem abgeschaltet. Auch linke Webseiten kennen jedoch den Streisand-Effekt: Die Wohnadresse von Til Schweiger ist seit dem Rechtsstreit auch bei anderen Online-Medien zu finden.

Update: Nachdem der Server gestern abgeschaltet wurde, ist er jetzt wieder da:

> On July 8th, 2014, members of the Cybrigade admin crew, as well as representatives of the Proledialers (call-centre workers, whose blog is hosted on espiv), went to the Panteion university premises. Their presence was enough to put the server back in operation.
>
> The attempted silencing of hundreds of collectives that use the espiv infrastructure was averted. Certainly, this does not mean that similar attempts by either the authorities or private individuals cannot occur in the future.

0

by Matthias Monroy at July 08, 2014 11:14 AM

Metalab

[alphabet] HeavyMeta on Tuesday 8 July 2014 - 20:00

https://metalab.at/wiki/HeavyMeta
(find some teasers through the link)

A mixture of music, cocktails, pan-cakes,
story-telling, beer, drawing and video
shall lure you to take a bite and have a sip or two.

Since it is on a weekday and it would (IMHO) be a nice opportunity
to introduce people to the lab, please do not expect to find
everybody there, but rather induce someone to come along!:-)

kind regards,
ktsouk

July 08, 2014 10:05 AM

Netzpolitik.org

World Intermediary Liability Map veröffentlicht

Welches Gesetz regelt eigentlich in Israel das Copyright? Solche und ähnliche Fragen stellt man sich des Öfteren, wenn man sich damit auseinandersetzt, was im Internet erlaubt ist und wer dafür zuständig ist, das zu koordinieren. Oft genug ist es schon schwer genug, im deutschen Regulierungsdschungel durchzusehen. Das Center for Internet and Society an der Stanford Law School hat einen Versuch unternommen, Licht ins Dunkel zu bringen und eine Landkarte erstellt, die internetrelevante Gesetzgebung, Entscheidungen und Behörden darstellt.

Ein schönes Projekt, doch leider gibt es noch ein paar weiße Flecken, vor allem bei amerikanischen Ländern. Aber an denen kann man mitarbeiten und über ein Formular (leider Google-Doc) neue Informationen hinzufügen oder allgemeines Feedback hinterlassen.

0

by Anna Biselli at July 08, 2014 08:11 AM

Dokumentation im Ersten: Zugriff! Wenn das Netz zum Gegner wird

Gestern um 22 Uhr lief im Ersten die Dokumentation "Zugriff!" in der dargestellt wird, wie die beiden Autorenkollegen Löbl und Onneken den Versuch unternehmen, sich auszuspionieren. Onneken ist dabei das "Opfer" und sieht sich dem Identitätsdiebstahl durch seine Kollegin ausgesetzt, verliert Zugriff auf seine Bankkonten, kann nicht mehr telefonieren und hat plötzlich eine rechtsgerichtete Zeitung abonniert. Leider werden nur Schreckensszenarien aufgebaut und keine Aussichten gegeben, wie und ob man sich wehren kann. Empfehlenswert vielleicht trotzdem, wenn man einem allzu Unbesorgten demonstrieren will, was prinzipiell machbar ist. Aber dann sollte man danach auch bereit sein, über mögliche Maßnahmen zur Vermeidung der heraufbeschworenen Situationen aufzuklären und das zu leisten, was die Doku leider verpasst.

Noch ein Jahr online verfügbar, die MP4-Datei zur Sicherung liegt hier.

0

by Anna Biselli at July 08, 2014 07:43 AM

AYFKMWTS? FBI goes Leetspeak

Auf MuckRock, in etwa das US-Pendant zu fragdenstaat.de, wurde eine Anfrage an das FBI gestellt und darum gebeten, Dokumentationen, Infomaterialien und anderes zur Interpretation von Leetspeak herauszugeben, die von der Geheimdienstbehörde FBI genutzt werden. Die Antwort kam in Form eines Twitter-Memos, das Übersetzungen von auf Twitter und anderen Social-Media-Kanälen üblichen Abkürzungen bereitstellen soll. Neben Klassikern wie “LMAO – laughing my a** off” (ja, Kraftausdrücke sind mit Sternchen dargestellt) gibt es auch allerlei absurdes wie “PMYMHMMFSWGAD - pardon me, you must have mistaken me for someone who gives a damn”. Aber gut zu wissen, womit sich die Intelligence Research Support Unit so beschäftigt. Hilft bestimmt beim Fangen von Terroristen auf Twitter, oder? Immerhin findet sich auch “STA – surveillance and target acquisition” unter den Abkürzungen. In der Einleitung spricht man aber von etwas ganz anderem:

> Diese Liste hat etwa 2800 Einträge und es wird Ihnen nützlich dabei sein, mit ihren Kindern und Enkelkindern mitzuhalten.

0

Flattr this!

by Anna Biselli at July 08, 2014 07:23 AM

July 07, 2014

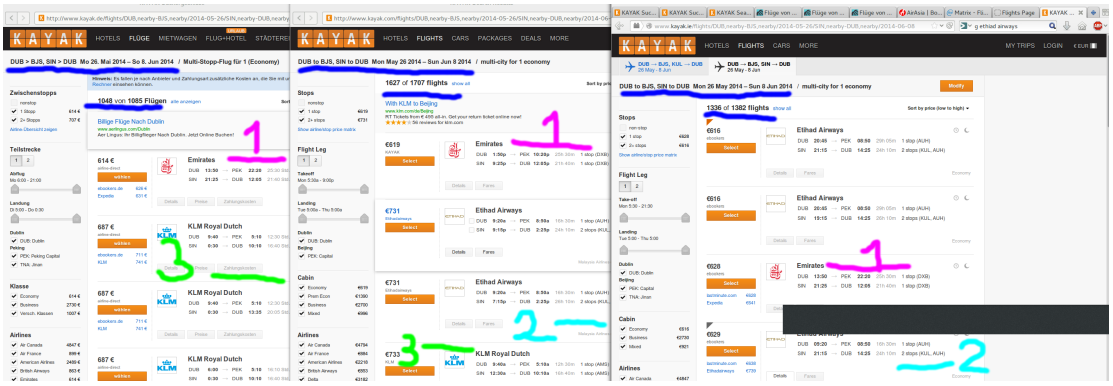
Muellis Blog

Finding (more) cheap flights with Kayak

People knowing me know about my weakness when it comes to travel itineraries. I spend hours and hours, sometimes days or even weeks with finding the optimal itinerary. As such, when I was looking for flights to GNOME.Asia Summit, I had an argument over the cheapest and most comfortable flight. When I was told that a cheaper and better flight existed that I didn’t find, I refused to accept it as I saw my pride endangered. As it turned out, there *were* more flights than I knew of.

Kayak seems to give you different results depending on what site you actually open. I was surprised to learn that.

Here is the evidence: (you probably have to open that with a wide monitor or scroll within the image)



In the screenshot, you can see that on the left hand side kayak.de found 1085 flights. It also found the cheapest one rated at 614 EUR. That flight, marked with the purple “1″, was also found by kayak.com and kayak.ie at different, albeit similar prices. In any case, that flight has a very long layover. The next best flight kayak.de returned was rated at 687 EUR. The other two Kayaks have that flight, marked with the green “3″, at around 730 EUR, almost 7% more than on the German site. The German Kayak does not have the Ethiad flight, marked with the blueish “2″, at 629 as the Irish one does! The American Kayak has that flight at 731 EUR, which is a whopping 17% of a difference. I actually haven’t checked whether the price difference persists when actually booking the flights. However, I couldn’t even have booked the Ethiad flight if I didn’t check other Kayak versions.

Lessons learnt: Checking one Kayak is not enough to find all good flights.

In addition to Kayak, I like to the the ITA Travel Matrix as it allows to greatly customise the queries. It also has a much more sane interface than Kayak. The prices are not very accurate though, as far as I could tell from my experiments. It can give you an idea of what connections are cheap, so you can use that information for, e.g. Kayak. Or, for that other Web site that I use: Skyscanner. It allows to list flights for a whole months or for a whole country instead of a specific airport.

What tools do you use to check for flights?

by muelli at July 07, 2014 07:09 PM

Netzpolitik.org

Nach US-Spionage: Bundesregierung plant, übliche 3-tägige Empörung auf 5 Tage auszuweiten

Der Postillion informiert: Nach US-Spionage: Bundesregierung plant, übliche 3-tägige Empörung auf 5 Tage auszuweiten.

> Drastisch wie noch nie will die Bundesregierung auf die neuesten Spionagevorwürfe gegen die USA reagieren. Wie das

> Kanzleramt am Montag mitteilte, habe man sich entschlossen, die sonst übliche dreitägige Empörung auf mindestens fünf Tage auszuweiten. Damit wolle man der eigenen Bevölkerung zwei Tage länger als üblich signalisieren, dass man nicht alles mit sich machen lasse.

0

Flattr this!

by Markus Beckedahl at July 07, 2014 03:37 PM

Potentieller Plagiator nutzt Copyright, um Untersuchung seiner Doktorarbeit zu verhindern

VroniPlag Wiki

Der Autor einer Dissertation hat die Plattform VroniPlag mit Hilfe einer sogenannten "DMCA-Notice" gezwungen, dass seine Doktorarbeit vorerst vom Netz genommen wurde. VroniPlag schreibt dazu:

> Aufgrund einer anwaltlichen DMCA-Notice[1] musste die Dokumentation umfangreicher Fremdtextübernahmen in dieser Hochschulschrift zunächst aus dem Wiki genommen werden.
>
> Das Abgeben einer falschen Erklärung im Zusammenhang mit einer solchen Maßnahme kann unter Umständen strafbar sein.
>
> Das Urheberrecht für plagiierte Texte in Anspruch zu nehmen, um eine DMCA-Notice zu versenden und die daraus folgenden juristischen Konsequenzen in Kauf zu nehmen, stellt eine bisher einmalige Vorgehensweise in der Zeit der Dokumentation von wissenschaftlichem Fehlverhalten auf dieser Plattform dar.
>
> Die weitere Vorgehensweise findet in enger Abstimmung mit Wikia, dem Betreiber des Wikis, statt.

Auf VroniPlag überprüfen Freiwillige Dissertationen auf Plagiate. Diese kollaborative Kontrollarbeit hat schon in mehreren Fällen dazu geführt, dass den betroffenen Plagiatoren ihr akademischer Grad wieder entzogen wurde, meistens weil zu große Teile der Arbeit wörtlich übernommen wurden, ohne ausreichend gekennzeichnet zu sein.

Auf diesen juristischen Winkelzug scheint bisher noch niemand gekommen zu sein. Eine DMCA-Notice bezieht sich auf den umstrittenen Digital Millenium Copyright Act aus den USA. Im Vergleich mit einer deutschen Abmahnung soll sie den Vorteil haben nicht direkt mit hohen Kosten für den betroffenen Betreiber einherzugehen. Allerdings ist es damit möglich amerikanische Anbieter, die ausländische Angebote hosten, zur Herausnahme von Texten zu bewegen. In diesem Fall ist es das kalifornische Unternehmen Wikia, das die Seite betreibt. Die Logik hinter der DMAC -Notice: zur Überprüfung der Promotion werden Zitate aus der wissenschaftlichen Arbeit übernommen, und diese seien urheberrechtlich geschützt.

VroniPlag will sich dem juristischen Druck aber anscheinend nicht kampflos ergeben. Die Argumentation wirkt auch etwas grotesk, denn so wären Plagiatoren mit möglichst vielen und großen "Fremdtextübernahmen" am stärksten vor der Überprüfung ihrer Arbeiten geschützt. Denn je mehr Plagiate es gibt, desto mehr Textauszüge müssen die freiwilligen Kontrolleure auf VroniPlag dokumentieren, was dann gegen amerikanisches Copyright verstieße. Hier scheint es rechtlichen Klärungbedarf zu geben, wie der DMCA mit den Fair-Use Bestimmungen in Einklang zu bringen ist. Diese erlauben nämlich die Nutzung geschützten Materials für bestimmte Zwecke.

Außerdem bleibt abzuwarten ob sich diese Art Abmahnung überhaupt für den (vermeintlichen) Plagiator lohnt, denn Dr. Sandro L. könnte unter Umständen auf diesem Weg wesentlich mehr Aufmerksamkeit auf seine Promotion lenken als ihm lieb ist. Wir sind gespannt welche Schritte Wikia als nächstes unternimmt.

0

Flattr this!

by Kilian Vieth at July 07, 2014 02:27 PM

Überwachung total – Rezension und Gespräch zum Buch

2007 hat der ehemalige Bundesdatenschutzbeautragte Peter Schaar sein Buch *Das Ende der Privatsphäre – Der Weg in die Überwachungsgesellschaft* veröffentlicht. In diesem Juni erschien sein neues Werk *Überwachung total – Wie wir in Zukunft unsere Daten schützen*.Was hat sich seitdem geändert, ist das Buch eine Fortsetzung oder musste nach Beginn der NSA-Affäre alles neu geschrieben werden? Und warum brauchen wir noch ein Buch zur Aufarbeitung der NSA-Enthüllungen, wo es doch bereits die überaus lesenswerten Werke von den Spiegelautoren Rosenbach/Stark und Glenn Greenwald gibt. Um das herauszufinden, haben wir uns das Schriftstück einmal angesehen und mit dem Autor geredet.

Peter Schaar sagt selbst, sein Buch sei sowohl eine Fortsetzung als auch ein Update des Vorgängers von 2007, die Grundstrukturen der Überwachung sind gleich geblieben, aber heute wisse man mehr als damals. Damals sei ihm in Rezensionen manchmal vorgehalten worden, er fokussiere sich zu stark auf die staatliche Rolle in der geheimdienstlichen Überwachung und deren Verwicklungen. Aber die Enthüllungen haben ihm Recht gegeben, ihn sogar noch übertroffen: “Heute weiß man, dass die Verknüpfung von Staat und Geheimdiensten sehr viel stärker ist.”

Mit seinen Ausführungen will Schaar nicht nocheinmal die Geschichte des Skandals erzählen und sich so detailliert und feingranular mit den Papieren auseinandersetzen wie Rosenbach und Stark das getan haben, die ihrerseits das Privileg besitzen selbst Zugang zu einem Teil der Dokumente zu haben. Der erste Teil des Buches – “Diagnose Totalüberwachung” kommt aber um eine Beschreibung der wichtigsten Dokumente und Programme der NSA-Überwachung nicht umhin. Doch abseits dieser Wiederholung, die man nicht unbedingt Zeile für Zeile lesen muss, wenn man die Thematik der letzten Monate interessiert mitverfolgt hat, sieht Schaar seine eigentliche Rolle im Einordnen der Erkenntnisse: “Ich setze die Snowden-Enthüllungen in einen technologischen Zusammenhang”. Und darin liegt auch die Stärke von Schaars Veröffentlichung, es geht nicht nur um die Überwachung durch die NSA. Schaar erklärt, welche Mechanismen des Internets Überwachung erst möglich machen und wie diese genutzt werden – nicht nur von Geheimdiensten. Er setzt sich auch mit anderen Gefahren für unsere Privatsphäre auseinander. Dabei fehlt Cloud Computing ebensowenig wie das SWIFT-Abkommen, Fluggastdatenabkommen, Vorratsdatenspeicherung und Anti-Terror-Listen, Themen die bei Rosenbach und Stark nicht weiter diskutiert werden.

Schaar findet an vielen Stellen deutliche Worte für das Verhalten der Bundesregierung. Mittlerweile kann er sich das erlauben, könnte man fast sagen. Denn heute ist er kein Bundesdatenschutzbeauftragter mehr, anders als noch 2007. Und auch wenn er sich bereits zu jener Zeit oft kritisch geäußert hat, eine Auseinandersetzung mit der deutschen Position wie in “Überwachung total” hätte damals wohl noch anders ausgesehen. Schaars neues Tätigkeitsfeld liegt bei der Europäischen Akademie für Informationsfreiheit und Datenschutz. Inhaltlich bleibt es also beim Datenschutz, aber nun kann er sich viel mehr für die Vernetzung mit der Zivilgesellschaft engagieren. “Ich wollte schon immer alle verschiedenen Stakeholder zusammenbringen.” Eine solcher ganzheitlicher Ansatz spiegelt sich auch in dem Lösungsansatz wieder, den Schaar im dritten Teil seines Buches vorschlägt. Es kann keinen Alleingang geben, sondern es muss auf vielen Punkten gearbeitet werden. An der Technik, an Gesetzen und an internationalen Abkommen. Das klingt nach einer schönen Idee, aber steht ein solcher Wunsch nicht auf überaus wackligen Beinen, wenn man betrachtet, wie wenige Konsequenzen in den letzten Monaten gezogen wurden und wie sich die Bundesregierung darum herum windet, klare Vereinbarungen mit den USA zu treffen?

> Die BRD muss ihr eigenes System und die Praktiken ihrer Nachrichtendienste kritisch überprüfen und ändern. Man kann nicht auf den Balken im Auge der USA zeigen und den eigenen ignorieren, sonst besitzt man keine Glaubwürdigkeit.

Aber nicht nur Deutschland müsse handeln, so Schaar, auch die EU müsse tätig werden, um global ernst genommen zu werden: “Man muss bei der Datenschutz-Reform darauf achten, dass man nicht durch die Cloud doch bei amerikanischen Stellen landet.”

Die wahrscheinliche Konsequenz: Eine Regionalisierung des Internets. Das ist keine schöne Vorstellung, doch Schaar fürchtet, dass es letztlich so kommen wird. “Lieber wäre mir ein gemeinsames Verständnis für Datenschutz. Auch gegenüber denen, die nicht im eigenen Land wohnen.”

Doch nicht nur auf internationaler Ebene ist es Zeit für Erneuerung, auch eine Reform der innerdeutschen Gesetze tut Not. In seiner Rolle als BDSB war Schaar oftmals mit Grenzen konfrontiert, die bei der Datenschutzaufsicht über deutsche Geheimdienste Schwierigkeiten bereiten. Wie bei Paragraph 24 des Bundesdatenschutzgesetzes, der eine Ausnahme formuliert:

> Personenbezogene Daten, die der Kontrolle durch die Kommission nach § 15 des Artikel 10-Gesetzes unterliegen, unterliegen nicht der Kontrolle durch den Bundesbeauftragten, es sei denn, die Kommission ersucht den Bundesbeauftragten, die Einhaltung der Vorschriften über den Datenschutz bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten.

Das heißt, dass nur die Prozesse der Datenverarbeitung der Kontrolle des BDSB unterliegen, nicht aber die Daten selbst. Um die müssen sich dann das Parlamentarische Kontrollgremium bzw. die G10-Kommission kümmern. “Aber nur das Gesamtbild ermöglicht eine Beurteilung. Niemand hat hier vollständigen Einblick.” – vor allem wenn Stellen wie das Innenministerium, das mit der Dienstaufsicht über den BDSB betraut ist, Informationen nur unvollständig oder gar nicht erst herausrücken. Die logische Folge: kontrollfreie Räume. Das bemängelte Schaar auch in einer Stellungnahme, die er im letzten November für die Bundesregierung erstellt hat sowie zuvor in seinem 24. Tätigkeitsbericht. “Reformen sind hier eine notwendige, aber keine hinreichende Bedingung”. Denn selbst die Möglichkeiten, die den Gremien heute gegeben sind, würden diese nicht ausreichend nutzen, kritisiert er. So sei er während seiner Amtszeit kein einziges Mal von der G10-Kommission darum gebeten worden, Datenverarbeitungsvorgänge zu untersuchen, wie es ihm laut dem obenstehenden Paragraphen auf Aufforderung möglich wäre. Eine logische Erklärung dafür zu finden ist schwer.

All die Ausführungen von Schaar zu notwendigen Aktualisierungen von Gesetzen, politischen und wirtschaftlichen Prozessen sind schlüssig, aber es wirkt ein bisschen wie eine naive Idealismusbrille, wenn man tagtäglich durch das Realverhalten politischer Entscheidungsträger desillusioniert wird. Aber sei es meinem politischem Pessimismus geschuldet oder der persönlichen Technikaffinität: Schaars Vorschläge auf technischer Seite sind eher in der Lage mich von ihrer Realisierbarkeit zu überzeugen. Telekommunikationsunternehmen konsequent dazu verpflichten, Ende-zu-Ende-Verschlüsselung zu nutzen und Daten nicht an andere Staaten weiterzugeben sowie die Entwicklung von Open-Source-Software zu fördern, transparenter zu machen und besser zu überprüfen – das klingt nach gangbaren ersten Schritten. Aber spätestens seit Sicherheitslücken wie Heartbleed ist auch klar: Open Source ist kein Allheilmittel – “Transparenz allein garantiert nicht, dass keine Überwachung stattfindet. Nur die Wahrscheinlichkeit, dass sie entdeckt wird, ist größer”.

Fazit: Überwachung total ist keineswegs eine bloße Verarbeitung des NSA-Skandal unter vielen. Das, was das Buch lesens- und empfehlenswert macht sind vor allem die Ausführungen zu dem, welche Überwachungsmechanismen auch ohne die NSA existieren - sei es staatlich, wirtschaftlich oder anderweitig motiviert. Denn die NSA-Affäre zeigt uns - wie Schaar im Gespräch mit Deutschlandfunk treffend feststellt – nur die Spitze des Eisbergs.

Wer das Buch erwerben will, kann das [*Disclaimer: Affiliate-Links, Klicken für Erklärung*] hier für Kindle (14,99) und hier in der Totholz-Ausgabe (17,99) tun.

0

by Anna Biselli at July 07, 2014 01:48 PM

Kontroverse Studie: Facebook spielt mit unseren Gefühlen

Eine kürzlich veröffentlichte Studie hat für großes Aufsehen gesorgt: ein bei Facebook angestellter Forscher hat gemeinsam mit zwei weiteren Wissenschaftlern eine experimentelle Studie verfasst. Darin wurden die Newsfeeds von 689.000 Facebook-Nutzern manipuliert um herauszufinden ob sich die Stimmung eines Nutzers auf andere überträgt. Dazu wurden verschiedenen Nutzergruppen gezielt mehr „positive“ bzw. „negative“ Beiträge angezeigt. Im Vergleich zu Testgruppen, deren Newsfeed-Algorithmus unverändert blieb, wurde dann untersucht ob sich die manipulierten Nutzer anders verhalten. Das wurde daran gemessen, was sie selbst auf Facebook posteten. Das Ergebnis der Forscher: Emotionen sind auf Facebook tatsächlich „ansteckend“. Wer mehr positive Beiträge sieht postet auch selbst mehr Positives. Markus hat das Experiment auch in seiner N24-Kolumne erklärt. Die wissenschafltiche Methodik der Studie wurde durchaus auch kritisiert. Uns interessieren aber vor allem die grundlegenden Fragen, ob solche Experimente überhaupt vertretbar sind und welche Konsequenzen sie haben.

Die Kontroverse: Dürfen die das?

Die aufgrund der Studie entbrannte Diskussion dreht sich um die Kernfrage, ob eine solche Studie ethisch vertretbar ist oder nicht. Zwischen wissenschaftlichen und unternehmerischen Ethikstandards klafft eine große Lücke. Wissenschaftliche Regeln sind aufgrund von Fällen schrecklichen Missbrauchs in der Vergangenheit wesentlich strikter, wie Ed Felten, Professor an der Princeton University, in seinem Artikel erklärt. Ein Unternehmen wie Facebook ist durch solche Regeln nicht gebunden.

Dürfen einfach Experimente mit Menschen gemacht werden, ohne sie vorab darüber aufzuklären, dass sie an einem Experiment teilnehmen? Hätten die Nutzerinnen und Nutzer nicht wenigstens vor den potentiellen Risiken des Experiments, z.B. für ihre psychische Gesundheit, gewarnt werden müssen?

Und für die Wissenschaft?

Ein Kritikpunkt an der Studie ist: die Forscher haben selbstständig darüber entschieden, wie und mit wem das Experiment durchgeführt wird. Das Einverständnis der Facebook-Nutzer wurde natürlich nicht abgefragt, bzw. einfach vorausgesetzt.

Viele wissenschaftliche Studien basieren jedoch auf Manipulation, die Probanden werden oftmals nur darüber aufgeklärt, dass es sich um eine Studie handelt. Es gibt aber auch Experimente, schreibt die Medienwissenschaftlerin Danah Boyd, bei denen absichtlich nicht vorab darüber informiert wird, dass es sich um ein Experiment handelt, weil das die Ergebnisse verfälschen könnte. Wo zieht man die Grenze? Ab wann kann man von einer Zustimmung ausgehen? Einfach Fragen scheint es darauf nicht zu geben.

Facebook hat für die Studie nichts anderes gemacht als auch sonst in seinem „Tagesgeschäft“, wie Boyd in ihrem Artikel anmerkt: Facebook manipuliert ständig den Newsfeed aller Nutzer und damit ihre Gefühle. Die Algorithmen zeigen stets nur eine Auswahl an Beiträgen, von denen man ausgeht, dass der Nutzer sie sehen will. Die Entscheidung was man im Newsfeed zu sehen bekommt und was nicht, basiert allerdings nicht auf transparenten Kriterien. Facebook ist für gewöhnlich eine Blackbox und mit der Studie ist nun ein winziger Teil dessen öffentlich geworden.

Warum betreibt und finanziert ein Unternehmen wie Facebook solche Forschung? Boyd meint: Sie wollen, dass wir glücklich sind. Denn wer mit einem guten Gefühl Facebook verlässt kommt gerne wieder. Die Manipulation gehört zum Geschäftsmodell.

Besser veröffentlichen als verheimlichen

Sollte Facebook keine wissenschaftlichen Studien mehr veröffentlichen? Das dürfte die generelle Problematik kaum lösen, meint Zeynep Tufekci, Professorin an der University of North Carolina, Chapel Hill:

> “The only real impact will be the disappointed researchers Facebook employs who have access to proprietary and valuable databases and would like to publish in Nature, Science and PNAS while still working for Facebook. Facebook itself will continue to conduct such experiments daily and hourly, in fact that was why the associated Institutional Review Board (IRB) which oversees ethical considerations of research approved the research: Facebook does this every day.”

Facebook kann seine Experimente auch im Verborgenen weiterführen, dann erfahren wir eben nur noch weniger darüber. Die Wissenschaft hat sicherlich ein Interesse sich einen Zugang zu Facebooks Daten und Programmen zu erhalten. Die Studie war eine

Forschungskooperation, die vom sogenannten Institutional Review Board (IRB), eine Institution die Forschungsvorhaben ethisch bewertet, genehmigt wurde. Dort schien man also kein Problem mit der Studie und der Art ihrer Durchführung gehabt zu haben.

Eine Machtfrage

Das die Studie nun eine Debatte darüber angestoßen hat, wie mit dieser Macht von Unternehmen wie Facebook umgegangen werden soll, war dringend notwendig. Wenn Facebook unsere Gefühle beeinflussen kann, dann wahrscheinlich auch unser Wahl- und Kaufverhalten. Doch was können wir tun? Facebook besser nicht verwenden, klar. Aber die Problematik liegt tiefer und ist natürlich nicht auf Facebook beschränkt. Jede große Internetplattform, genauso wie Regierungen, spielen das Spiel mit und investieren in die Erforschung und Steuerung des Nutzerverhaltens, wie Tufekci betont:

> "And of course it's not just Facebook, every major Internet platform, along with governments, are in this game and they are spending a lot of money and effort because this is so important."

Im Grunde geht es also in der aktuellen Debatte um die Facebook-Studie nicht um die Studie sondern vielmehr um die wachsende Kritik am Geschäftsmodell von Firmen wie Facebook, das auf der Sammlung und Nutzung von Daten beruht. Der berühmte Satz auf der Facebook-Startseite, der Dienst sei kostenlos und werde es auch immer bleiben, stimmt eben nicht. Zeynep Tufekci und Tal Yarkoni diskutieren diesen Punkt sehr engagiert in einem CNN Interview (auf Englisch). Wozu Facebook und andere Dienste in der Lage sind, könne man nicht mit klassischer Marktforschung vergleichen, denn der Einfluss und die Reichweite seien deutlich umfassender und tiefgreifender, als bei „konventionellen" Marketingmethoden. Denn Facebook arbeite unsichtbar und wisse viel mehr über seine Nutzer als klassische Werbefachleute. Andere Studien zeigen zum Beispiel, dass Facebook auch das Wahlverhalten beeinflussen kann.

Es gehe in der Debatte also nicht in erster Linie um Forschung, sondern um Macht. Die Macht zu bestimmen wie mit Nutzerdaten umgegangen werden soll.

Wie reagieren?

Danah Boyd schlägt die Einrichtung von "Ethik-Beiräten" vor, die nicht nur von den Unternehmen selbst, sondern auch mit Nutzern und Wissenschaftlern besetzt werden sollen. Sicherlich eine diskussionswürdige Idee. Aber der Druck für solche Initiativen muss von unten, von den Kunden kommen. Wer gibt schon freiwillig seine Macht ab? Nur wenn die großen Anbieter sich ernsthaft durch den Vertrauensverlust der Nutzerinnen und Nutzer bedroht sehen, werden sie bereit sein zu handeln. Die Diskussion um die Studie ist ein plakatives Beispiel, doch die grundlegende Frage darf darüber nicht vergessen werden, ganz egal ob es als „Forschung" oder „Marketing" bezeichnet wird.

0

Flattr this!

by Kilian Vieth at July 07, 2014 12:27 PM

Grimme Online Award für netzpolitik.org – Das Video von der Preisverleihung

Auf den Gewinn eines Grimme-Online-Awards in der Kategorie Spezial hatten wir schon hingewiesen. Jetzt ist auch der Ausschnitt der Preisverleihung in Köln auf Youtube veröffentlich worden. Für uns war Kirsten Fiedler vor Ort, um den Preis abzuholen. Dort war sie genauso überrascht wie wir, was sie von der Preispatin zu hören bekam:

(Die ersten 3:20 Minuten kann man sich sparen, wenn man kein Fernsehen schaut. Die witzigste Stelle beginnt um 4:50).

0

Flattr this!

by Markus Beckedahl at July 07, 2014 11:23 AM

#DNP14 – Daten, Netz & Politik in Wien

Die österreichischen Kollegen von unwatched.org veranstalten am 20. und 21. September zum dritten Mal einen Netzpolitik-Kongress in Wien. Dieses Jahr steht unter dem Motto "Brandung 2.0" und das Programm verspricht viele interessante Vorträge unter anderem rund um Datenschutz, Urheberrecht, Digitale Selbstverteidigung und Informationsfreiheit. Der Ticketverkauf hat begonnen und ihr seid herzlich eingeladen, euch mit den netzpolitisch Aktiven aus unserem Nachbarland zu vernetzen und auszutauschen!

0

Flattr this!

by Anna Biselli at July 07, 2014 09:36 AM

UEFA will verbesserte Verfahren zur Videoüberwachung in Stadien diskutieren

Aufnahme eines Stadions in Südafrika vom EU-Satellitenzentrum EUSC und dem deutschen DLR.

Die UEFA will die Sicherheit in Fußballstadien erhöhen, indem verstärkt Soziale Medien genutzt werden sollen. Dies geht aus einem Protokoll einer EU-Ratsarbeitsgruppe hervor, die sich mit Strafverfolgung beschäftigt. Demnach hat die belgische Delegation hierzu eine Präsentation gehalten. Ob die Internetdienste dabei lediglich zur Verbreitung von Informationen genutzt werden sollen, wird nicht berichtet. Möglich wäre auch, Soziale Medien gezielt zu analysieren um Rückschlüsse auf das Verhalten von Fans zu ziehen. Das Bundesinnenministerium ist an Forschungen zu Anwendungen beteiligt, die anhand von Nachrichten bei Twitter Prognosen für die Sicherheit entwerfen sollen. Hierfür wird unter anderem die Funktion des Geo-Tagging von Tweets genutzt: So kann festgestellt werden, wenn sich Nachrichten mit bestimmten Inhalten in der Umgebung von Stadien häufen.

Die Entwicklung entsprechender Verfahren wird auf der jährlichen Konferenz zu Stadionsicherheit thematisiert. Jeweils zum Start einer Saison treffen sich hierzu die Sicherheitsbeauftragten der Nationalverbände, "Sicherheitsmanager" der Stadien, Sicherheitsbeauftragte der Klubs sowie Angehörige von Polizeibehörden. Letztes Jahr wurde die Konferenz von 350 Teilnehmenden besucht. Laut der UEFA spiegele die Anzahl die "gewachsene Tragweite von Stadien- und Sicherheitsfragen" wider.

Anwendungen von Siemens in Brasilien

Auf der nächsten Konferenz, die vom 10. bis 12. September in Warschau stattfinden soll, sollen auch verbesserte Verfahren zur Videoüberwachung auf der Tagesordnung stehen. Auch dies geht aus dem Dokument hervor. Die Kameras sollen hinsichtlich eines "crowd managements" genutzt werden. Auch hierzu werden keine näheren Angaben gemacht.

Hinsichtlich der Ausrüstung von Stadien in Brasilien hatte der Elektronikkonzern Siemens verlautbart, Stadien mit entsprechender Technik ausgerüstet zu haben. Auf der Webseite von Siemens heißt es zur Funktionsweise der "umfassenden Lösungen für Videoüberwachung", jeder Winkel des Veranstaltungsorts könne damit überwacht werden. Ausschreitungen und Überfüllung in den Gängen würden sofort erkannt. Die Systeme stünden mit automatischen Ticketkontrollen "in Verbindung". Dadurch würde "bekannten Hooligans" der Zugang verwehrt.

Der Spiegel berichtete zur Europameisterschaft 2012 in Polen, die Stadien seien mit Gesichtserkennungssystemen ausgerüstet gewesen. Die Zahl der Kameras sei beträchtlich erhöht worden, ihre Auflösung sei "so hoch, dass sie auf 220 Meter Entfernung Nasenhaare in einem Gesicht erkennbar machen können".

Die UEFA arbeitet zur Stadionsicherheit mit der Europäischen Union und dem Europarat zusammen. 2007 wurde ein "UEFA-/EU-Arbeitsprogramm" gestartet, drei Jahre später wurde das Programm nach Beschluss des UEFA-Exekutivkomitees und des Rates der Europäischen Union ausgeweitet. Die UEFA lobt diese "öffentlich-private internationale Partnerschaft" als "in ihrer Art und ihrem Ausmaß einmalig".

Firma in Katar mittlerweile Marktführer

Auch das "International Centre for Sport Security" (ICSS) befasst sich mit mehr Stadionsicherheit. Die Firma wurde vom früheren DFB-Sicherheitsbeauftragten Helmut Spahn gegründet. Laut dem "Spiegel" habe es das ICSS geschafft, "den internationalen Sport-Sicherheitsmarkt völlig umzukrempeln". Spahn habe beispielsweise die Zuschläge für die Sicherheitsplanung und -betreuung der Fußball-Weltmeisterschaften 2018 in Russland und 2022 in Katar erhalten. Auch die Olympischen Winterspiele in Sotschi 2014 wurden vom ICSS begleitet, die Sommerspiele 2018 sollen folgen. Die Firma betreue auf diese Weise "beinahe alle internationalen Top-Veranstaltungen der kommenden zehn Jahre".

Der "Spiegel" zitiert einen nicht namentlich genannten Verbandspräsidenten "eines großen Sportdachverbands"sowie einen "Fifa-Insider". Beide argwöhnen, dass es bei der Auftragsvergabe an das ICSS Unregelmäßigkeiten gegeben habe. Ein Indiz dafür sei der Sitz der Firma in Katar.

0

Flattr this!

by Matthias Monroy at July 07, 2014 09:23 AM

CCC Hamburg

Themenabend: "Angewandte Konsensdemokratie" & "Firmen besser machen"

In zwei Vorträgen widmen wir uns der Frage, wie man im 21. Jahrhundert Firmen betreibt und dem miteinander abseits der klassischen Hierarchieformen. Als Referenten freuen wir uns auf @blackspear und @luebbermann es wird ausreichend Raum für Diskussionen geben.

Dienstag, 08.07.14 ab 20:00

by dodger at July 07, 2014 08:39 AM

Netzpolitik.org

De Maizières Datenschutzinitiative: Alter Wein in neuen Schläuchen? Wir veröffentlichen die Original-Vorschläge

Thomas de Maizière.
Foto: MC1 Chad J.
McNeeley. CC BY 2.0.

In der vergangenen Woche hat Bundesinnenminister Thomas de Maizière seine "Initiative zur Datenschutz-Grundverordnung" gestartet. Diese besteht aus einem Schreiben an die aktuelle griechische und kommende italienische Ratspräsidentschaft sowie EU-Justizkommissarin Viviane Reding und der Ankündigung mit Wirtschaft, Wissenschaft und Zivilgesellschaft in einen Dialog treten zu wollen. Das Schreiben enthält sechs Punkte, die das Innenministerium als "Kernfragen" bezeichnet, "die bislang eine Einigung im Rat verhindert hatten". Anders gesagt: Es handelt sich dabei vor allem um jene Punkte, mit denen die Bundesregierung ihre Verzögerung der Verhandlungen in Brüssel legitimiert hat.

Da das Innenministerium die Vorschläge lediglich in einer Pressemitteilung umreißt, veröffentlichen wir an dieser Stelle die Original-Vorschläge, die das Innenministerium verschickt hat:

- Anlage zum Schreiben des Herrn Ministers an GRC- und ITA-Vorsitz: Vorschlag für eine Roadmap zur Beschleunigung der Verhandlungen über die EU-Datenschutzreform (DE)
- Annex to Federal Minister de Maizière's letter to the Greek and Italian Presidencies Proposed roadmap to speed up the negotiations on EU data protection reform (ENG)

Einordnung der Initiative

Was ist nun von den Vorschlägen de Maizières zu halten? Zunächst einmal kann die EU-Datenschutzverordnung als eine der wichtigsten (netz)politischen Großbaustellen Aufmerksamkeit und Initiative vertragen. Die geltende Datenschutzrichtlinie stammt aus dem Jahr 1995 und ist kaum durchsetzungsfähig, während der informationstechnische "Fortschritt" weiter Tatsachen schafft. In diesem Sinne ist das Schreiben des Innenministers zu begrüßen.

Dabei darf man jedoch nicht vergessen, dass de Maizière nicht der erste deutsche Innenminister ist, der die EU-Datenschutzreform zur Priorität *erklärt*. Auch de Maizières Vorgänger Friedrich beherrschte rhetorische Spielchen zur Datenschutzreform – wenn auch vielleicht nicht auf dem gleichen Level wie sein Nachfolger, der sich in seiner Rolle als Internetversteher sichtlich gefällt. Auch ein zivilgesellschaftlicher Dialog wurde im vergangenen Jahr noch unter Friedrichs Ägide ins Leben gerufen, verlief dann allerdings nach wenigen Treffen im Sande.

Die Vorschläge im Einzelnen

Schauen wir also auf die 6 Punkte, die de Maizière prioritär behandeln will, um im Rat zu einer Einigung zu gelangen. Im Überblick: 1. Rechtsform und höhere Datenschutzstandards im öffentlichen Bereich; 2. Konkretisierung der Voraussetzungen der Einwilligung; 3. „One Stop Shop"; 4. Drittstaatenübermittlungen; 5. Big Data und Profiling; 6. Meinungs- und Informationsfreiheit.

1. Rechtsform und höhere Datenschutzstandards im öffentlichen Bereich: Kernpunkt dieses Absatzes ist der Vorschlag, eine Öffnungsklausel für die Datenverarbeitung im öffentlichen Bereich einzuführen, die es Mitgliedsstaaten erlaubt, "über die Bestimmungen der Datenschutz-Grundverordnung hinauszugehen und strengere nationale Datenschutzbestimmungen zu erlassen [...]".

Eine Öffnungsklausel scheint zunächst die bessere Option als auf eine Ausklammerung des öffentlichen Bereichs in der Verordnung zu pochen, wie es Deutschland länger getan und somit die ganze Verordnung gefährdet hat. Zudem stand diese Position der des Europäischen Parlaments, verschiedener Mitgliedsstaaten und der Kommission diametral gegenüber.

Auf der anderen Seite lassen sich hier vier Nachteile skizzieren: 1. Die Öffnungsklauseln sind wahrscheinlich nicht Konsens – weder im Ministerrat, noch im Parlament – und könnten somit für weitere Verzögerung sorgen. Mit den Öffnungsklauseln könnte eine neue, zeit- und kraftraubende Debatte im Rat eröffnet werden. 2. Mitgliedsstaaten mit einem niedrigen Datenschutzniveau im öffentlichen Sektor (Ja, die gibt es und das ist ein Problem!) bleiben weiterhin im Regen stehen, wenn das garantierte Mindestniveau nichts wert ist und die Öffnungsklausel zu locker ausfällt. 3. Das deutsche Datenschutzrecht im öffentlichen Bereich ist fragmentiert und weist durchaus Reformbedarf auf, um den sich Deutschland nicht drücken sollte. Ein richtungsweisendes Gutachten dazu datiert auf das Jahr 2001.

Was man diesem Punkt zugutehalten muss: Es handelt sich hier bei um einen konkreten, neuen Vorschlag.

Das kann man vom Punkt **2, Konkretisierung der Voraussetzungen der Einwilligung,** nicht vollends behaupteten. Alles, was de Maizière hier anspricht, wird seit über zwei Jahren diskutiert und dürfte weitestgehend Konsens sein – zumindest in Kommission und Parlament. Einzig beim Punkt der "Konkretisierung dieser Voraussetzungen der Einwilligung für bestimmte Situationen" horcht man auf, und hofft, dass hier keine Schlupflöcher ihren Weg in die Datenschutzverordnung finden.

Die Ausführungen zu Punkt **3, „One Stop Shop"**, dem Wie und Was der Zusammenarbeit der Datenschutzbehörden in Europa, kann

ich juristisch nicht bewerten. Hinweise dazu gerne in den Kommentaren. Fakt ist: Es braucht starke nationale Datenschutzbehörden und einen starken Europäischen Datenschutzausschuss, der für eine europaweit einheitliche Auslegung der Verordnung sorgt. Das darf weder ein Widerspruch, noch zu teuer, noch zu bürokratisch sein. Spezifisch neu ist an de Maizières Punkt, so scheint es, erstmal nichts. Deutschland beharrt auf einem Vorschlag, den es bereits eingebracht hat.

Die **Drittstaatenübermittlungen** (Punkt 4), genauer gesagt die "Anti-Fisa-Klausel", hat Kirsten hier schon kommentiert. Weder der Vorschlag, noch dass Deutschland eine solche Klausel unterstützt, ist eine Neuigkeit. Zu der vorläufigen Einigung über die Drittstaatenübermittlungen im Rat, auf die sich das Schreiben bezieht, fehlt bislang eine vollständige Analyse aus bürgerrechtlicher Sicht. Auch Hinweise dazu nehmen wir gerne in den Kommentaren entgegen.

5. Big Data und Profiling: Die angeblich fehlende "Internettauglichkeit" der Datenschutzverordnung ist, neben dem öffentlichen Bereich, bislang das zweite deutsche Hauptargument gegen eine Einigung im Rat (vgl. exemplarisch).

Auch in diesem Absatz ist nichts zu entdecken, was nicht jeder in Europa formal so unterschreiben würde und nicht schon Teil des Verordnungsvorschlags wäre. Das Argument, dieser wäre nicht "internettauglich" entkräftet das Innenministerium somit unfreiwillig selbst:

> Ich trete daher dafür ein bewährte Instrumente wie die Einwilligung zu stärken und erforderlichenfalls zusätzliche Schutzmechanismen vorzusehen. Darüber hinaus müssen den Betroffenen effektive Auskunftsansprüche zur Verfügung stehen, um Entscheidungen, die – wie etwa eine Bewertung der Kreditwürdigkeit – auf Profilen beruhen, nachvollziehen zu können.

"Zusätzliche Schutzmechanismen" nennt der Innenminister nicht. Ein solcher könnte z.B. eine Registrierungspflicht für bestimmte Verfahren der Datenverarbeitung sein, wie es ein Kurzgutachten von iRights.law zum Verbraucher-Tracking vorschlägt.

Aufhorchen lässt allerdings der Satz:

> Sie (Informationspflichten und Einwilligungserfordernisse; B.B.) stoßen jedoch an Grenzen, wenn die Information der Betroffenen erst deren Identifizierung verlangt, wodurch ein zusätzliches Datenschutzproblem entsteht.

Das könnte in sensiblen Ohren wie Rhetorik zur Legitimation von Schlupflöchern bei Informationspflichten und Einwilligungserfordernissen klingen.

6. Meinungs- und Informationsfreiheit: Hier spricht de Maizière das "Google-Urteil" des EuGH an, über dessen Auswirkungen und Anwendung heftig diskutiert wird – auch auf netzpolitik.org. Die Idee, dass Unternehmen wie Google über die Ausgestaltung nicht allein entscheiden sollten, sondern "unabhängige Schiedsstellen", ist eine Überlegung wert. Konkreter wird de Maizière allerdings nicht.

Generell ist darauf zu achten, dass diese Stellen wirklich unabhängig agieren. Ein Modell wie der industrienahe Selbstregulierung Informationswirtschaft e.V. (SRIW), der bislang vor allem beim Häuserverpixeln hilft, ist keine Option.

Fazit: Konsequenzen abwarten

Eine Initiative ist laut Duden ein "erster tätiger Anstoß zu einer Handlung; erster Schritt bei einem bestimmten Handeln". Betrachten wir das Vorschlagen einer Agenda im Rat in diesem Sinne, ist de Maizières Initiative ihren Namen wert. Auf der anderen Seite finden sich wenig konkrete neue Vorschläge in de Maizières Diskussionspunkten. Im schlimmsten Fall ist diese "Initiative" ein neuer Anstrich der deutschen Verzögerungstaktik im Rat, was ich dem Innenministerium nicht pauschal unterstellen will. Schließlich ist Initiative das, was viele seit langem von der Bundesregierung fordern. Was davon konkret zu halten ist, müssen die nächsten Leaks aus der Blackbox Ministerrat zeigen.

0

by Benjamin Bergemann at July 07, 2014 07:26 AM

Mit leerem Akku in die USA reisen heißt Terrorismusgefahr

Aus der Kategorie April-Scherz könnte die Bekanntgabe der amerikanischen Behörde Transportation Security Administration stammen, wenn sie nicht so traurig wäre: Wer von ausgewählten ausländischen Flughafen – um welche es sich handelt, wurde nicht bekannt gegeben – in die USA fliegt, muss seine elektrischen Geräte beim Boarding angeschaltet lassen. Wenn nicht, muss mit zusätzlichen Sicherheitsuntersuchungen gerechnet werden. Als offizielle Begründung soll wie immer Terrorgefahr herhalten, denn in Smartphones, Laptops und Co. könne man immerhin ausgezeichnet Bomben verstecken.

Weiterführender Vorschlag: Warum nicht gleich vorschreiben, dass Gerätepasswörter deaktiviert sein und alle persönlichen Daten beim Einchecken auf einen amerikanischen Server übertragen werden müssen? Nur um sicherzugehen, falls beim Screening unzähliger unschuldiger Bürger doch mal jemand durchs Raster gefallen sein sollte.

0

by Anna Biselli at July 07, 2014 06:28 AM

BND wird durch Spion infiltriert – Scheinempörung und "Lösungsvorschläge"

Mittlerweile sind die Zweifel weitgehend ausgeräumt, dass der BND-Mitarbeiter, der letzte Woche Schlagzeilen als vermeintlicher Spion gemacht hat, wirklich für US-Geheimdienstbehörden gearbeitet hat. Im Zuge dessen soll er über einen Zeitraum von zwei Jahren sensible Informationen aus dem BND in die USA weitergegeben haben. Eine Wetter-App, die im Hintergrund verschlüsselte Kommunikation aufbaut, ein USB-Stick mit BND-Interna und konspirative Treffen in Österreich verhärten den Verdacht.

Der Fall ist wieder einmal eine weitere Spitze in den NSA-Verwicklungen, aber das eigentlich Erschreckende im Fall ist wieder einmal, wie unsere führenden Politiker und Repräsentanten (nicht) reagieren. Ein Best-Of halbherziger Empörungsversuche und Lösungsvorschläge:

Starten wir mit Kanzlerin Angela Merkel. Die verweilt derzeit noch in China zu Regierungsgesprächen und der Erkundung des lokalen Markttreibens. Stellungnahmen haben Zeit. Die Kölnische Rundschau titelt "Merkel findet keine Worte". Doch heute morgen gab es laut der Wirtschaftswoche eine Regung der Kanzlerin. Sie sei besorgt, habe sie auf einer Pressekonferenz in Peking gesagt und stellt fest: Es "handelt sich [...] um einen sehr ernsthaften Vorgang". Aber keine Sorge, der Generalbundesanwalt prüft den Fall bereits. Und wir wissen ja schon, wie das ausgeht, denn der ermittelt jetzt auch hinsichtlich der Ausspähung des Kanzlerinnen-Handys - während es für den Rest der Bevölkerung wohl noch nicht für eine Klage reicht.

Regierungssprecher Steffen Seibert nominiert sich selbst für den "Captain Obvious"-Award:

> Die Sache ist ernsthaft, ist doch klar.

Das hat auch Ex-US-Außenministerin Hillary Clinton erkannt:

> Das ist ganz klar ein ernstes Thema [...] Wir sind in einer Phase, in der wir anfangen müssen, einige Linien zu ziehen

Bundespräsident Joachim Gauck wird leicht deutlicher, wobei uns das stark an die "Ausspähen-unter-Freunden-geht-ja-gar-nicht"-Rhetorik erinnert :

> Dann ist ja nun wirklich zu sagen: Jetzt reicht's auch einmal.

Hans-Peter Uhl von der CSU bläst in ein ähnliches Horn:

> Die Amerikaner halten sich ganz offenkundig nicht daran, dass man Verbündete nicht ausspäht [...] Sie führten sich in Deutschland auf "wie eine digitale Besatzungsmacht."

Innenminister de Maizière gibt vor, immer noch daran zu glauben, zusammen mit den USA Aufklärung zu erlangen:

> Der Vorwurf selbst wiegt sehr schwer. Die Vorfälle müssen jetzt zügig aufgeklärt werden. Erst dann können wir das Ausmaß der *mutmaßlichen* Spionage einschätzen. Ich erwarte jetzt eine schnelle, eindeutige Äußerung der Vereinigten Staaten von Amerika.

Vermutlich hat er da eine ähnlich zeitnahe Stellungnahme im Sinn wie diejenige, die unsere Bundesregierung bereits seit letztem Jahr "fordert". Daher kann de Maizière auch bedenkenlos konkrete Schritte auf den St. Nimmerleinstag nach der Antwort der USA verschieben:

> Konsequenzen daraus möchte ich erst treffen und mit meinen Kollegen beraten, wenn die Amerikaner sich eindeutig geäußert haben.

Aber keine Sorge, untätig wird der Minister nicht bleiben. Die Lösung liegt klar auf der Hand – einfach die eigenen Geheimdienste aufrüsten und als Nebeneffekt auch alle anderen besser überwachen:

> Zunächst zeigt der Vorwurf [...] dass eine effiziente und wirksame Spionageabwehr gegenüber *Jedermann* wichtig, notwendig und auch noch besser als bisher zu organisieren ist.

Ähnliches berichtet auch die BILD-Zeitung und beruft sich dabei auf ein Papier des Innenministeriums laut dem Gegenmaßnahmen geplant würden und der Aufklärungsauftrag der deutschen Dienste erweitert werden solle. De Maizière habe auch in einer "internen Runde" gesagt, man müsse einen 360°-Blick bekommen. Diese Linie unterstützt auch der innenpolitische Sprecher der Union im Bundestag:

> Der Fall des BND-Agenten zeigt: Wir müssen auch unsere vermeintlichen Verbündeten stärker im Fokus haben.

Außenminister Steinmeier lud letzten Freitag den US-Botschafter ins Auswärtige Amt, um ihm zu sagen, dass die USA zu einer zügigen Aufklärung beitragen sollten und berichtet nun aus der Mongolei:

> Wenn die Berichte zutreffen, dann reden wir hier nicht über Kleinigkeiten [...] Deshalb müssen die USA mit ihren Möglichkeiten an einer schnellstmöglichen Aufklärung mitwirken. Aus Eigeninteresse sollten die USA dieser Mitwirkungspflicht auch Folge leisten.

Worüber sollte man sich eigentlich mehr aufregen? Über die Untätigkeit der zuständigen Politiker oder darüber, dass sie ernsthaft

anzunehmen scheinen, die Bevölkerung weiterhin glauben machen zu können, man wolle noch an irgendeiner Stelle Konsequenzen ziehen?

0

Flattr this!

by Anna Biselli at July 07, 2014 05:57 AM

July 06, 2014

CCC Dresden

Themenabend Open Source und Faire IT

Datum
Freitag, 11. Juli 2014 um 19:00 Uhr bis 20:30 Uhr
Ort
GCHQ, Lingnerallee 3

Im Zeitraum vom Mai bis Juli diesen Jahres möchte das Team vom Sukuma Award Dresden Workshops, Infostände usw. zum Thema "nachhaltige Globalisierung" veranstalten, welche als Inspiration für die Teilnehmer des Wettbewerbs dienen sollen. Dabei hat sich das Team auch an das Chaos macht Schule-Projekt gewandt und einen Themenabend zu "Open Source" vorgeschlagen, welchen wir auch gern durchführen möchten.

Da dieses Event jedoch nicht nur exklusiv für die Teilnehmer des Sukuma Award-Wettbewerbs stattfinden soll, laden wir hiermit alle dazu ein, die sich für das Thema interessieren und gern zur Diskussion beitragen möchten! Eintritt frei!

by CCC Dresden (mail@c3d2.de) at July 06, 2014 03:36 PM

Themenabend Open Source und Faire IT

Datum
Freitag, 11. Juli 2014 um 19:00 Uhr bis 20:30 Uhr
Ort
GCHQ, Lingnerallee 3

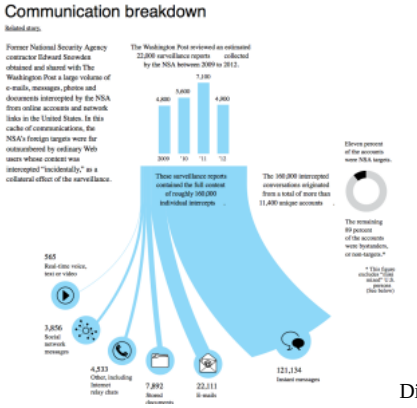
Im Zeitraum vom Mai bis Juli diesen Jahres möchte das Team vom Sukuma Award Dresden Workshops, Infostände usw. zum Thema "nachhaltige Globalisierung" veranstalten, welche als Inspiration für die Teilnehmer des Wettbewerbs dienen sollen. Dabei hat sich das Team auch an das Chaos macht Schule-Projekt gewandt und einen Themenabend zu "Open Source" vorgeschlagen, welchen wir auch gern durchführen möchten.

Da dieses Event jedoch nicht nur exklusiv für die Teilnehmer des Sukuma Award-Wettbewerbs stattfinden soll, laden wir hiermit alle dazu ein, die sich für das Thema interessieren und gern zur Diskussion beitragen möchten! Eintritt frei!

by CCC Dresden (mail@c3d2.de) at July 06, 2014 03:36 PM

Netzpolitik.org

Washington Post bekommt NSA-Cache von Snowden mit konkreten Überwachungsdaten



Die Waschington Post berichtet über NSA-Überwachungsdaten, die Edward Snowden kopiert und den Journalisten zur Verfügung gestellt hat. Erstmals geht es nicht um konkrete Überwachungsprogramme, sondern um die Datensätze, die damit gespeichert worden sind. Wie zu erwarten: Sehr viele Unschuldige fallen ins Raster. In NSA-intercepted data, those not targeted far outnumber the foreigners who are.

Die Datensätze stammen aus einem FISA-Cache und sollten gesondert geschützt sein. Darunter fallen 160.000 überwachte eMail- und Instant-Messaging-Gespräche, eine davon hunderte Seite lang und 7900 Dokumente von ingsgesamt mehr als 11.000 Online-Accounts. Ein von neun Datensätzen soll was mit konkreten Verdächtigen zu tun haben, acht von neun Datensätze stammen von unschuldigen Bürgern, die einfach nur Pech hatten. Um diese alle zu ermitteln musste man auch erstmal alles überwachen, um diese rausrastern zu können. Wie man sich das vorstellen kann, funktionierte es auch nicht, US-Bürger händisch oder maschinell rauszufiltern. (Der BND soll ja .de-Mailadressen automatisch rausfiltern und damit die Verfassung achten).

> Many other files, described as useless by the analysts but nonetheless retained, have a startlingly intimate, even voyeuristic quality. They tell stories of love and heartbreak, illicit sexual liaisons, mental-health crises, political and religious conversions, financial anxieties and disappointed hopes. The daily lives of more than 10,000 account holders who were not targeted are catalogued and recorded nevertheless.

Was man berücksichtigen sollte: Die Washington Post interessiert sich vor allem für die Frage, wieviele US-Bürger als Unschuldige überwacht wurden. Unschuldige Nicht-US-Bürger waren für die Frage weniger relevant.

Die offiziellen Überwachungszahlen wird man wohl korrigieren müssen:

> In a June 26 “transparency report,” the Office of the Director of National Intelligence disclosed that 89,138 people were targets of last year’s collection under FISA Section 702. At the 9-to-1 ratio of incidental collection in Snowden’s sample, the office’s figure would correspond to nearly 900,000 accounts, targeted or not, under surveillance.

Noch im Mai hatte der ehemalige NSA-Chef General Keith Alexander erklärt, dass Edward Snowden auf keinen Fall auf solche Überwachungsdaten haben zugreifen können und lügen würde, wenn er das behauptet. Jetzt wurde Keith Alexander erneut einer Lüge überführt.

Ein Problem der Snowden-Enthüllungen war bisher, dass es sich eher um Beschreibungen von Überwachungsprogrammen handelte, was vielen zu unkonkret und threoretisch war. Im vergangenen Herbst gab es eine Diskussion darüber, ob das in unserem Politikfeld mit Tschernobyl für die Umweltbewegung vergleichbar sei. Dafür spricht einiges, vor allem die riesige mediale Aufmerksamkeit, wenn auch die Öffentlichkeit an sich etwas zurückhaltend agiert. Mittlerweile bin ich eher überzeugt, dass es noch davor einzuordnen sei, ähnlich einem Atomwissenschaftler, der mit Bauplänen an die Öffentlichkeit geht und erklärt, was bei einem GAU passieren könnte. Mit anderen Worten: Hätten wir die Verbindungsdaten von Angela Merkels Handy über drei Ebenen oder gar die Transcripte der Telefonate, dann wäre es konkreter und fassbarer für viele, was es bedeutet, dass Angela Merkel abgehört wird. Insofern ist es zu begrüssen, dass es mittlerweile konkreter wird.

Apropos anlasslose Überwachung: Wie hat eigentlich unser Verfassungsschutz die Mail gefunden, die der mutmaßliche BND-Doppelagent der russischen Botschaft zwecks Angebots geschrieben haben soll?

0

Flattr this!

by Markus Beckedahl at July 06, 2014 07:51 AM

July 05, 2014

Netzpolitik.org

NSA-Untersuchungsausschuss: Zur Sicherheit Musik

Der Verfassungsschutz hat Bundestagsabgeordnete und Mitglieder des NSA-Untersuchungsausschuss davor gewarnt, dass diese “mit einer gezielten Überwachung rechnen” müssten. Dafür gibts jetzt Kryptohandys und die Abgeordneten können in Büros wechseln, die mit Wände mit Aluminiumplatten ausgestattet sind. Allerdings wären die Büros dann nicht mehr in ihre Fraktionsgemeinschaften integriert.

Interne Besprechungen im NSA-Untersuchungsausschuss finden dann auch ohne Handies statt und mit Musik, z.B. Edvard Griegs Klavierkonzert in a-Moll. Das und mehr steht in einem Artikel bei sueddeutsche.de: NSA-Untersuchungsausschuss: Zur Sicherheit Musik.

> Ein BND-Mitarbeiter soll für die USA spioniert haben – dabei sind die Amerikaner eigentlich Partner der deutschen Geheimdienste. Doch inzwischen ist das Misstrauen der deutschen Parlamentarier so groß, dass sie nur unter ungewöhnlichen Sicherheitsvorkehrungen über die NSA beraten.

0

Flattr this!

by Markus Beckedahl at July 05, 2014 02:28 PM