erschienen in der FIfF-Kommunikation,
herausgegeben von FIfF e.V. - ISSN 0938-3476
www.fiff.de

Stefan Hügel

Log 2/2012

Ereignisse, Störungen und Probleme der digitalen Gesellschaft

Immer wieder gibt es Ereignisse, Verlautbarungen und Entscheidungen, die im Zusammenhang mit dem fortschreitenden Abbau von Bürgerrechten stehen. Wir dokumentieren hier einige davon. Die Aufzählung ist sicherlich nicht vollständig; mit einigen besonders bedeutsamen Ereignissen wollen wir aber auf die weiterhin besorgniserregende Entwicklung hinweisen.

Februar 2012

12. Februar 2012: Der Bundesdatenschutzbeauftragte Peter Schaar sieht bei der staatlichen Software zur Überwachung von Computern Datenschutzanforderungen als nicht erfüllt an. Der vom Bundesverfassungsgericht geforderte Schutz des Kernbereichs privater Lebensgestaltung werde verletzt. Schaar hatte die Software geprüft, die vom Bundeskriminalamt, vom Zollfahndungsamt und von der Bundespolizei eingesetzt worden war. Die Frage, ob die in der Software enthaltene Nachladefunktion bereits rechtswidrig sei, ließ er dabei zunächst offen (Quelle: Heise).

13. Februar 2012: Dem Bericht eines ehemaligen Mitarbeiters eines Pharmadienstleisters zufolge haben Rechenzentren in Deutschland illegal mit Daten aus Apothekenrezepten gehandelt. Die Daten seien an Kunden aus der Pharmaindustrie verkauft worden. Es sei dadurch nachvollziehbar gewesen, welche Medikamente von welchen Arztpraxen verschrieben worden seien (Quelle: Heise).

14. Februar 2012: Einem Bericht des Wall Street Journal zufolge hatten Hacker aus China jahrelang Zugriff auf die Systeme des Telekom-Unternehmens Nortel. Sie nutzten dabei offenbar gestohlene Passwörter von Managern des Unternehmens, die ihnen von 2000 bis zur Entdeckung 2004 weitgehenden Zugang zu technischer Dokumentation, Entwicklungsberichten, Geschäftsplänen und E-Mail ermöglicht hätten. Identifiziert worden seien die Angreifer nicht; sie hätten aber anscheinend von China aus operiert (Quelle: Wall Street Journal, Heise).

15. Februar 2012: Auch die iOS- und Android-Anwendungen Twitter, Foursquare und Foodspotting übertragen unter bestimmten Umständen das Adressbuch des jeweiligen Nutzers an den Hersteller. Twitter hat bestätigt, dass die Daten hochgeladen und für 18 Monate gespeichert würden, wenn der Nutzer in der Anwendung nach Freunden sucht. Ähnliches gilt für Foursquare und Foodspotting. Teilweise würden die Daten sogar ungesichert übertragen (Quelle: Los Angeles Times, netzpolitik.org, Heise).

16. Februar 2012: Der Europäische Gerichtshof (EuGH) entscheidet, dass die Durchsuchung von auf Webservern gespeicherten Benutzerdaten nicht mit EU-Recht vereinbar ist. Die belgische Verwertungsgesellschaft Sabam hatte dies von einem Provider gefordert. Das Gericht begründet die Entscheidung damit, dass eine solche Anordnung den Anbieter zu einer unzulässigen allgemeinen Überwachung verpflichten würde (Quelle: netzpolitik.org).

20. Februar 2012: Im Rahmen eines Prozesses vor dem Amtsgericht in Reutlingen hat der Richter den Facebook-Account des Angeklagten beschlagnahmt, um Zugriff auf dessen Daten zu bekommen. Experten zufolge ist das ein Novum in einem deutschen Gerichtsprozess. Das Gericht erwartet daraus Hinweise zu einem Wohnungseinbruch (Quelle: Heise).

20. Februar 2012: Mit dem Communications Capabilities Development Programme (CCDP) will die britische Regierung Telekom-Provider zu einer verschärften 12-monatigen Vorratsdatenspeicherung verpflichten. Sicherheitsbehörden sollen in Echtzeit Zugriff auf die gespeicherten Daten von Kommunikationsvorgängen erhalten. Die konservativ-liberale Regierung hatte nach ihrem Wahlsieg noch angekündigt, die unter der Labour-Regierung auf den Weg gebrachte Vorratsdatenspeicherung zu begrenzen (Quelle: Daily Telegraph, netzpolitik.org, Heise).

21. Februar 2012: Zwei kanadische Hochschulen haben einen Vertrag mit der Lizensierungsgesellschaft Access Copyright abgeschlossen, mit denen der Vereinigung von Universitätslehrern zufolge eine umfassende Überwachung verbunden ist. Die Nutzung und Nutzungshäufigkeit geschützter Werke sollen kontrolliert werden; dies mache laut der Canadian Association of University Teachers (CAUT) neue Instrumente erforderlich. Die Datenschutzbestimmungen seien demgegenüber lächerlich (Quelle: Heise).

24. Februar 2012: Das Bundesverfassungsgericht hat entschieden, dass die Regelungen zur Speicherung und Herausgabe von Nutzerdaten, Passwörtern und PIN-Codes an Behörden teilweise gegen das Grundrecht auf informationelle Selbstbestimmung verstoßen und damit verfassungswidrig sind. Die Praxis, § 113 TKG für Auskünfte über den Inhaber einer IP-Adresse heranzuziehen, stelle einen Eingriff in das Fernmeldegeheimnis dar. Datenschützer begrüßen die Entscheidung (Quelle: Bundesverfassungsgericht, Heise).

24. Februar 2012: Die Gesellschaft für Informatik kritisiert das Abkommen ACTA. Patent- und markenrechtliche Fragen könnten Vorrang vor den Bürgerrechten bekommen, so die Standesorganisation der Informatiker. Ein Fragenkatalog zu ACTA wurde an das Wirtschafts- und das Justizministerium gesendet (Quelle: Heise).

24. Februar 2012: Digitale Bürgerrechtsorganisationen in den USA wenden sich gegen einen Gesetzentwurf zur Einführung einer einjährigen Vorratsdatenspeicherung. Es gehe darum, einen „weiteren Angriff der Regierung auf das Internet und seine Nutzer zu stoppen", so der Direktor der Organisation Demand Progress (Quelle: Heise).

25. Februar 2012: Die deutschen Geheimdienste haben im Jahr 2010 nach einem Bericht des Parlamentarischen Kontrollgremiums (PKG) rund 37 Millionen Netzverbindungen überwacht. Die Überprüfung erfolgte aufgrund von ca. 16.400 Schlüsselwörtern wie beispielsweise „Bombe". Die Zahl der überwachten Verbindungen hat sich damit mehr als verfünffacht. Hinweise ergaben sich dabei lediglich in 213 Fällen. Grüne und FDP kritisieren den Anstieg der Überwachung und fordern, die Suchkriterien zu präzisieren. Das Bundeskanzleramt verteidigt die Überwachung; wesentlicher Grund für den massiven Anstieg sei die Zunahme von Spam (Quelle: Bild, netzpolitik.org, Heise).

März 2012

1. März 2012: Finanzbehörden in Niedersachsen haben mit einem Sammelauskunftsersuchen bei Amazon Händlerdaten in großem Umfang angefordert. Sie forderten eine bundesweite Liste von Händlern, deren Jahresumsätze die Grenze von 17.500 Euro übersteigen. Eine Klage von Amazon gegen das Ersuchen war in erster Instanz erfolgreich; Grund dafür sei aber lediglich der Umstand, dass die Daten bei Amazon in Luxemburg gelagert sind (Quelle: Spiegel, Heise).

1. März 2012: Trotz Protesten wegen massiver Datenschutzbedenken führt Google seine Dienste zusammen. In der neuen Datenschutzerklärung werden die Richtlinien für mehr als 60 Dienste vereinheitlicht und die Möglichkeit geschaffen, Nutzerdaten gesammelt auszuwerten. Aus Sicht der französischen Datenschutzkommission CNIL verstoßen die Regelungen gegen europäisches Recht. Auch Bundesverbraucherschutzministerin Ilse Aigner kritisiert die neuen Regelungen: „Mit der Zusammenlegung der Daten hat das Unternehmen eine Kehrtwende vollzogen und alle Bedenken europäischer und US-amerikanischer Datenschützer ignoriert" (Quelle: Heise).

2. März 2012: Der Deutsche Bundesrat verlangt die Ausweitung der „Verbunddatei Rechtsextremismus". Die Datei berücksichtige nicht ausreichend die Belange des Verfassungsschutzes, um das Nachrichtendienstliche Informationssystem der Verfassungsschutzbehörden von Bund und Ländern (NADIS) als Analyseinstrument zu nutzen. Es fehlten Informationen zur übergreifenden Erkennung von Netzwerkstrukturen (Quelle: Heise).

6. März 2012: Berichten britischer Medien zufolge ist die Klage der Internetserviceprovider British Telecom und TalkTalk gegen die in der britischen Digital Economy Bill (DEA) vorgesehenen Internetsperren endgültig gescheitert. Nachdem der High Court in London die Beschwerde bereits vergangenes Jahr zurückgewiesen hatte, wurde nun auch die Berufung gegen diese Entscheidung abgelehnt. Das Gesetz sieht Sanktionen bei Urheberrechtsverletzungen bis hin zur Sperrung des Internetanschlusses vor (Quelle: Heise).

8. März 2012: In den Niederlanden wird der BigBrotherAward von der Bürgerrechtsorganisation Bits of Freedom verliehen. Ausgezeichnet werden die niederländische Regierung und das Internetunternehmen Facebook. Die niederländische Polizei erschien bei der Gala in Amsterdam um ihren Preis abzuholen, der ihr für den Einsatz von Trojanersoftware verliehen wurde (Quelle: bigbrotherawards.nl, Heise).

12. März 2012: Die Überwachung des Internet im Iran und in China wurde deutlich verstärkt, stellt der Bericht Feinde des Internet der Organisation Reporter ohne Grenzen fest. In China werde starker Druck auf Internetunternehmen ausgeübt; der Iran wolle ein abgeschottetes, „nationales Internet" errichten. Der Bericht nennt zwölf Staaten als „Feinde des Internet"; darunter neben China und Iran auch Syrien, Kuba, Nordkorea, Saudi-Arabien und weitere Staaten. Unter Beobachtung stehen unter anderem Frankreich und Australien (Quelle: Reporter ohne Grenzen, Heise).

16. März 2012: Gegen 18 IT-Unternehmen reichen texanische Anwälte eine Sammelklage wegen Ausspähens privater Daten ein. Es geht dabei unter anderem um Betreiber von Social Networks und Spieleanbietern, die sich die Adressbuchdateien ihrer Nutzer über mobile Anwendungen verschaffen. Unter den Beklagten sind die Unternehmen Apple, Electronic Arts, Facebook, Foursquare, LinkedIn und Twitter (Quelle: Heise).

16. März 2012: Die NSA errichtet in Utah eine neues Cyberspionage-Center. Nach einem Bericht von Wired sollen alle Arten von Kommunikationsvorgängen, einschließlich privater E-Mails, Mobiltelefonate, Suchanfragen und alle weiteren Arten digitaler Spuren, wie z. B. Parkquittungen oder Buchkäufe überwacht werden. Wired sieht in dem Zentrum eine Umsetzung des offiziell 2003 gestoppten „Total Information Awareness"-Programms (TIA) aus der Bush-Ära (Quelle: Wired, netzpolitik.org).

27. März 2012: Das National Counter Terrorism Center (NCTC) soll nach einer neuen Richtlinie Informationen über US-Bürger, die nicht unter Terrorismusverdacht stehen, künftig nicht mehr nach 180 Tagen löschen. Stattdessen sollen die Daten künftig fünf Jahre aufbewahrt und ausgewertet werden. Damit will die US-Regierung verstärkt Daten Unverdächtiger für Terrorbekämpfung nutzen. Bürgerrechtler ziehen erneut Vergleiche zum früheren „Total Information Awareness"-Programm (Quelle: Heise).

28. März 2012: Aus Sicht des Berliner Datenschutzbeauftragten Alexander Dix sind die Risiken der Datenverarbeitung dramatisch gestiegen. Er führt das auf neue Überwachungstechniken in Staat und Wirtschaft zurück. Durch die Kompromittierung von Sicherheitsdiensten wie der SSL-Zertifikate von Diginotar drohe „eine ganze Infrastruktur der Kommunikation zusammenzubrechen". Vor einer besonderen Herausforderung stehe das Datenschutzrecht, da große Unternehmen wie Google, Facebook, Apple oder Amazon immer größere Datensammlungen anlegten. Personenbezogene Daten würden dabei rechtswidrig in die USA übermittelt; ihre Nutzung sei nicht zulässig (Quelle: Berliner Beauftragter für Datenschutz und Informationsfreiheit, Heise).

30. März 2012: Der österreichische Arbeitskreis Vorratsdatenspeicherung (AK Vorrat) reicht beim österreichischen Verfassungsgerichtshof (VfGH) Verfassungsklage ein. Die zum 1. April 2012 in Kraft tretende Vorratsdatenspeicherung soll für verfassungswidrig erklärt und aufgehoben werden (Quelle: netzpolitik.org, Heise).

April 2012

1. April 2012: Bei der Anwendung der in Österreich neu in Kraft getretenen Vorratsdatenspeicherung wird von verschiedener Seite das Datenschutzgesetz verletzt, da die erforderlichen Genehmigungen der Datenschutzkommission teilweise noch nicht vorliegen oder gar nicht beantragt wurden. Darauf weist die österreichische Gesellschaft für Datenschutz Arge Daten hin. Betroffen ist auch das Verkehrsministerium (Quelle: Heise).

2. April 2012: Über eine Sicherheitslücke beim Zahlungsabwickler Global Payments haben sich Angreifer bis zu 1,5 Millionen Kreditkartennummern verschafft. Dies wurde von dem Unternehmen bestätigt. Das Problem sei inzwischen unter Kontrolle. Betroffen sind Mastercard- und Visa-Kreditkarten (Quelle: Heise).

2. April 2012: In Großbritannien werden Pläne für eine massive Internet-Überwachung konkretisiert. Provider hätten nach dem Entwurf Hardware zu installieren, die der britischen Behörde GCHG eine plattformübergreifende Beobachtung individueller Kommunikation erlaubt. Zeitpunkt, Position der Teilnehmer und Dauer sollen langfristig gespeichert werden und in Echtzeit verfolgbar sein. Dem Telegraph zufolge bestätigte ein Sprecher des britischen Innenministeriums (Home Office) die Existenz solcher Pläne, erklärte jedoch, es handele sich dabei nur um notwendige Anpassungen und sei unumgänglich (Quelle: New York Times, Telegraph, netzpolitik.org, Heise).

4. April 2012: In Polen wurden 2011 1,86 Millionen Verbindungs- und Standortinformationen durch Strafverfolgungsbehörden abgefragt – 2010 waren es noch 1,38 Millionen, 2009 ca. 1 Million Fälle. Polnische Behörden dürfen die Vorratsdaten nicht nur, wie in der EU-Richtlinie vorgesehen, für die Verfolgung schwerer Straftaten, sondern auch zur Gefahrenabwehr nutzen. Die Genehmigung durch einen Richter ist nicht erforderlich (Quelle: Panoptykon Foundation, Heise).

4. April 2012: Die Bundesregierung sieht keinen Handlungsbedarf angesichts der geringen Anzahl von Internet-Nutzern mit niedrigem Einkommen. Dies erklärt sie zu einer Anfrage der Fraktion der Linken. Die stellvertretende Vorsitzende der Linksfraktion, Halina Wawzyniak erklärt dazu, die Bundesregierung sei blind gegenüber der sozialen Spaltung (Quelle: Heise).

10. April 2012: Der Iran will laut einem Bericht der International Business Times ausländische Webseiten nur noch sehr eingeschränkt zugänglich machen. Ab August sollen dem iranischen Minister für Informations- und Kommunikationstechnik zufolge alle iranischen Internet-Service-Provider nur noch den Zugang zu einem „Nationalen Internet" zulassen. Betroffen sind beispielsweise Such- und E-Mail-Dienste wie Google, Hotmail und Yahoo. Sie sollen durch eigene Dienste in einem iranischen „Intranet" ersetzt werden (Quelle: International Business Times, netzpolitik.org, Heise).

10. April 2012: Ein Gesetzentwurf gegen Cyberkriminalität in den USA wird von Bürgerrechtlern kritisiert. Im Cyber Intelligence Sharing and Protection Act (CISPA) soll der Datenaustausch zwischen staatlichen Stellen wie Geheimdiensten oder Ermittlungsbehörden und dem Privatsektor geregelt werden. Der Geheimdienstausschuss des Repräsentantenhauses hat den Entwurf bereits angenommen. Kritiker fürchten, dass das Gesetz in dieser Form schwerwiegendere Auswirkungen als die inzwischen auf Eis gelegten Gesetzentwürfe SOPA und PIPA haben könnte (Quelle: Heise).

11. April 2012: Nachdem im vergangenen Jahr Schulbuchverlage einen speziellen Trojaner zum Aufspüren von Plagiaten im Bildungsbereich einsetzen wollten, löst nun eine Ersatzmaßnahme bei Lehrervereinigungen Proteste aus. Die niedersächsische Landesschulbehörde fordert von Schulleitern beispielsweise eine Erklärung, dass auf Rechnern ihrer Einrichtungen keine rechtswidrig angefertigten digitalen Kopien analoger Lehrmaterialien gespeichert sind. Die Schulen sollen Berichten zufolge in diesen Tagen eine „Erinnerung mit detaillierten Informationen" erhalten (Quelle: Neue Osnabrücker Zeitung, Heise).

13. April 2012: In Bielefeld werden die deutschen Big Brother Awards 2012 verliehen. Preisträger sind dieses Mal unter anderem Bundesinnenminister Friedrich, der sächsische Innenminister Ulbig und die Unternehmen Brita und Electronic Arts. Positive Erwähnung fand der schleswig-holsteinische Datenschutzbeauftragte Thilo Weichert (vgl. auch Seiten 16-22; Quelle: BigBrotherAwards.de, netzpolitik.org, Heise).

16. April 2012: Der Bundesbeauftragte für den Datenschutz, Peter Schaar, hat sich davon überzeugt, dass die personenbezogenen Daten aller rund 35 Millionen Arbeitnehmer für das System des Elektronischen Entgeltnachweises (Elena) nun auch physisch

gelöscht sind. Es handelt sich um rund 700 Millionen Datensätze, die bei der früheren Zentralen Speicherstelle und der Registratur Fachverfahren gespeichert waren. Schaar hatte bereits im Dezember 2011 sämtliche Schlüssel vernichtet und die Daten damit unzugänglich gemacht (Quelle: netzpolitik.org, Heise).

18. April 2012: Die US-Regierung kritisiert den Entwurf zum Cyber Intelligence Sharing and Protection Act (CISPA). Jedes Gesetz für einen besseren Schutz des Cyberspace müsse Regelungen für einen strikten Datenschutz und verbindliche Sicherheitsstandards für wichtige Infrastruktur wie das Stromnetz und die Wasserversorgung enthalten (Quelle: The Hill, Heise).

19. April 2012: Das europäische Parlament stimmt dem umstrittenen neuen transatlantischen Abkommen zum Transfer von Passenger Name Records (PNR) mit 409 Ja- und 226 Nein-Stimmen zu. Die Daten dürfen damit weiterhin 15 Jahre in den USA gespeichert werden. Anonymisiert können die Informationen der Fluggesellschaften sogar unbegrenzt aufbewahrt werden. Schwerpunktmäßig sollen damit terroristische und schwere Kriminalität bekämpft werden; US-Behörden können aber immer auf PNR zugreifen, wenn auf die verfolgte Straftat in den Vereinigten Staaten drei Jahre Haft stehen – damit beispielsweise auch bei Diebstahl (Quelle: netzpolitik.org, Heise).

19. April 2012: Bundeskanzlerin Angela Merkel (CDU) hat ihre Minister aufgefordert, schnell die EU-Vorgaben zur Vorratsdatenspeicherung zu erfüllen. „Die Richtlinie als solche liegt auf dem Tisch und sie muss umgesetzt werden", sagte Merkel laut dpa (Quelle: Deutsche Presse-Agentur, Heise).

22. April 2012: Ariane Friedrich, Hochspringerin und Polizeibeamtin, veröffentlicht auf Facebook Namen und Wohnort eines Mannes, der ihr eine anzügliche E-Mail mit angehängtem Foto geschickt haben soll. Sie habe das Foto nicht angesehen; es solle sich dabei um eine Abbildung des Geschlechtsteils des Senders handeln. Anderen Angaben zufolge handele es sich um die Abbildung eines Pudels. Die Bekanntgabe löst öffentliche Diskussionen über die Rechtmäßigkeit dieses Vorgehens aus (Quelle: Spiegel Online, Wikipedia).

24. April 2012: Der Europäische Datenschutzbeauftragte Peter Hustinx warnt vor einer Bedrohung der Privatsphäre und des Datenschutzes durch das Abkommen ACTA. Viele der Maßnahmen zur Verstärkung der Durchsetzung von geistigen Eigentumsrechten könnten eine breit angelegte Überwachung des Verhaltens und der Kommunikation von Nutzern beinhalten und tief in die Privatsphäre von Individuen eingreifen. Unterschiedslose oder breit angelegte Überwachung des Verhaltens und/oder der Kommunikation von Internetnutzern in Bezug auf geringfügige, nicht profit-orientierte Verstöße wären nicht verhältnismäßig und würden gegen Artikel 8 der EMRK, Artikel 7 und 8 der Grundrechtecharta und die Datenschutzrichtlinie verstoßen (Quelle: netzpolitik.org).

27. April 2012: Das US-amerikanische Repräsentantenhaus stimmt mit 248 zu 168 Stimmen für den Cyber Intelligence Sharing and Protection Act (CISPA). Durch den Austausch von Informationen über Bedrohungen zwischen Unternehmen und Behörden soll die Netzinfrastruktur besser geschützt werden. Zu dem Gesetz wurden einige Ergänzungen angenommen, unter anderem eine präzisere Festlegung, auf welche Informationen die Bundesbehörden Zugriff erhalten dürfen (Quelle: netzpolitik.org, Heise).

27. April 2012: Die Innenminister der EU einigen sich darauf, dass Passenger Name Records (PNR) zwei Jahre „unmaskiert" gespeichert werden sollen. Der ursprüngliche Entwurf für eine Richtlinie der EU-Kommission sah eine Anonymisierung der Daten bereits nach 30 Tagen vor. Insgesamt sollen die Informationen fünf Jahre lang vorgehalten werden können (Quelle: europa.eu, netzpolitik.org, Heise).

30. April 2012: Nach einem Bericht des Nachrichtenmagazins Der Spiegel soll in hessischen Filialen des Discounters Aldi Kundinnen in kurzen Röcken oder mit tief ausgeschnittenen Tops heimlich gefilmt worden sein. Filialleiter hätten mit Überwachungskameras herangezoomt, wenn sich die Kundinnen über Kühltheken beugten oder vor Regalen bückten (Quelle: Spiegel, Heise).

Mai 2012

1. Mai 2012: Der Bundesbeauftragte für den Datenschutz, Peter Schaar, fordert die Bundesregierung auf, die Möglichkeiten zur Videoüberwachung von Arbeitnehmern stärker einzuschränken. Schaar begrüßt das geplante Verbot heimlicher Videoüberwachung, sieht aber die im Entwurf vorgesehene Möglichkeit der offenen Videoüberwachung als „Öffnungsklausel" und damit besonders kritisch – insbesondere, da sie auch zur Qualitätskontrolle eingesetzt werden kann. Schaar befürchtet im Ergebnis eine Ausweitung der Videoüberwachung am Arbeitsplatz (Quelle: Der Bundesbeauftragte für den Datenschutz, Heise).

2. Mai 2012: Die beiden Polizeibeamten, die auf der Demonstration „Freiheit statt Angst" im September 2009 in Berlin einen Radfahrer misshandelten, werden nach der Aussage des Anwalts der Nebenklage wegen einfacher Körperverletzung im Amt zu einer Geldstrafe von jeweils 120 Tagessätzen verurteilt (Quelle: Heise).

5. Mai 2012: Nach Vorstellung des FBI sollen Anbieter von Internet-Diensten Abhörschnittstellen für Dienste wie soziale Netze, VoIP-Telefonie, Instant-Messaging und E-Mail einrichten. Dies sei bei einem Treffen mit Vertretern von Google, Yahoo, Facebook und weiteren Anbietern diskutiert worden (Quelle: CNet, Wired, Heise).

10. Mai 2012: Das FBI und weitere Strafverfolgungsbehörden wollen eine Vorratsdatenspeicherung für Domain-Registrare durchsetzen. Gespeichert werden sollen Kunden-Bestandsdaten und Verkehrsdaten zu einer Domain (Quelle: Heise).

14. Mai 2012: Das Zugangsrecht zu Akten des Brüsseler Verwaltungs- und Regierungsapparates soll eingeschränkt werden. Bisher seien „jegliche Inhalte unabhängig von ihrer Medienart" unter die Informationsfreiheit gefallen, so die britische Bürgerrechtsorganisation Statewatch. Sämtliche Entwürfe oder Diskussionspapiere des Rats, der Kommission und des Parlaments würden durch die neuen Regelungen der Öffentlichkeit vorenthalten, fürchtet Statewatch-Direktor Tony Bunyan (Quelle: Statewatch, Heise).