INTERNET ARCHIVE WaybackMachine
http://www.klicksafe.de/themen/datenschutz/grundlagenwissen/wo-hinterlasse-icl Go
4 captures
7 Nov 12 - 13 Jul 13
DEZ JUL AUG
2012 2013 2014
13
Close
Help

klicksafe.de
Die EU-Initiative für mehr Sicherheit im Netz

Wo hinterlasse ich Spuren im Netz?

1. Der Staat als Datensammler
2. Firmen als Datensammler
3. Soziale Netzwerke und der Datenschutz

Schaut man sich an, wo wir alltäglich Datenspuren hinterlassen, so entkommen wir kaum der Welt von Videokameras, Kreditkarten, Rabatt- oder Kundenkarten, Telefonverbindungen und Internetprotokollen. Daran haben Firmen mit wirtschaftlichem Interesse an unseren Daten einen großen Anteil.
Einen spannenden Animationsfilm zum Thema Datenspuren, der sich auch zur Einführung des Themas in den Unterricht eignet, finden Sie unter: http://panopti.com.

- **Anmerkung:** Die Vorratsdaten-Speicherpflicht beläuft sich nicht, wie im Film erwähnt, auf 2 Jahre, sondern umfasst ein halbes Jahr!

1. Der Staat als Datensammler

Vorratsdatenspeicherung
Die Vorratsdatenspeicherung ist in Deutschland durch das „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ eingeführt worden und trat am 1. Januar 2008 in Kraft.

Vorratsdatenspeicherung bezeichnet hier die Verpflichtung der Anbieter von Telekommunikationsdiensten zur Registrierung von elektronischen Kommunikationsvorgängen, ohne dass ein Anfangsverdacht oder konkrete Hinweise auf Gefahren, wie z.B. eine terroristische Bedrohungssituation, bestehen. Kommunikationsinhalte sind von dieser Pflicht nicht betroffen, es müssen ausschließlich sog. „Verbindungsdaten” erfasst und ein halbes Jahr lang gespeichert werden.

- **Anmerkung:** Ein Urteil am **2. März 2010** des deutschen Bundesverfassungsgerichts besagt, dass die Vorratsdatenspeicherung in Deutschland in ihrer bisherigen Umsetzung verfassungswidrig ist. Mehr zur Vorratsdatenspeicherung bei Wikipedia.

Anbieter von Telefondiensten einschließlich Mobilfunk- und Internet-Telefondiensten (wie bspw. Skype) speichern:

- Rufnummern, Anrufzeit, bei Internet-Telefondiensten auch die jeweilige IP-Adresse, bei SMS auch indirekt den Standort durch Speicherung der Mobilfunkzelle. Dies gilt für die Daten des Anrufers aber auch des Angerufenen bzw. für Absender und Empfänger!

E-Mail-Diensteanbieter (wie gmail, gmx, freenet etc.) speichern:

- IP- und Mailadressen von Absender und Empfänger und Zeitpunkte jedes Zugriffs auf das Postfach.

Anbieter von Internetzugangsdiensten speichern:

- IP-Adresse, Datum und Uhrzeit des Verbindungsaufbaus mit dem Internet

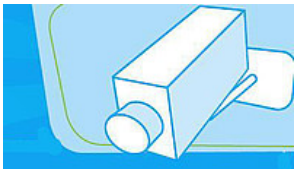
Kurz und gut: Während der Beamte einer Strafverfolgungsbehörde nicht hören darf, WAS Sie sagen (den Inhalt), so weiß er doch sehr genau, WANN Sie mit WEM WIE LANGE und WO Sie kommuniziert haben.

Öffentliche Kritik
Die „Vorratsdatenspeicherung“ wird als umstrittenste Datensammelmaßnahme der vergangenen Jahre bezeichnet. Als Begründung für das Gesetz wird angeführt, die Speicherung diene der Bekämpfung der organisierten Kriminalität und der Terrorabwehr. Die Vorratsdatenspeicherung ist verfassungsrechtlich nicht unumstritten, „da sie anlasslos in die Grundrechtspositionen sämtlicher Nutzer elektronischer Dienste eingreift. Zudem würde die für eine freiheitliche Gesellschaft konstitutive unbefangene Kommunikation erheblich beeinträchtigt“, so die Position der Konferenz der Datenschutzbeauftragten des Bundes und der Länder.
Denn mithilfe der über die gesamte Bevölkerung gespeicherten Daten könnten:

- Bewegungsprofile erstellt,
- geschäftliche Kontakte rekonstruiert
- und Freundschaftsbeziehungen identifiziert werden.

Auch Rückschlüsse auf

- den Inhalt der Kommunikation,
- auf persönliche Interessen und
- die Lebenssituation der Kommunizierenden werden möglich.



Zugriff auf die Daten haben Polizei, Staatsanwaltschaft und ausländische Staaten, die sich davon eine verbesserte Strafverfolgung versprechen. Es wurde bereits 2007 Verfassungsbeschwerde gegen das Gesetz eingereicht und eine endgültige Entscheidung wird vom Bundesverfassungsgericht bis dato erwartet. Bis dahin ist die Nutzung der allein aufgrund dieser neuen gesetzlichen Pflicht gespeicherten Daten nur zur Verfolgung schwerer Straftaten erlaubt.
Der Verdacht muss in diesem Fall

- durch bestimmte Tatsachen begründet sein und
- die Erforschung des Sachverhaltes auf andere Weise wesentlich erschwert oder unmöglich sein.

Weitere Informationen zum Thema Vorratsdatenspeicherung in Deutschland: www.vorratsdatenspeicherung.de

Was ist eine IP-Adresse?
Eine IP-Adresse (IP: Abkürzung für engl. „Internet-Protocol”) ist so etwas wie die Rufnummer im Telefonnetz, nur für das Internet. Sie erlaubt die eindeutige Adressierung von Rechnern (und anderen Geräten) in IP-basierten Datennetzen. Daher bekommen alle im Internet angeschlossenen Rechner eine IP-Adresse zugewiesen. Praktisch handelt es sich dabei um einen mehrstelligen Zahlencode, der zumeist aus vier durch Punkte voneinander getrennten Zahlen zwischen 0 und 255 besteht.

Tipp: auf www.wieistmeineip.de bekommen Sie Ihre aktuelle IP-Adresse angezeigt.(Quelle: Handreichung Datenschutz, mekonet kompakt)

Chipkarten und Ausweise

Der Staat betätigt sich nicht nur bei der Telekommunikation als Datensammler, auch andere Systeme wie Chipkarten und Ausweise ermöglichen die digitale Verarbeitung persönlicher Daten. Genannt seien hier vor allem die biometrischen Daten in elektronischen Ausweispapieren. Die besondere Problematik der maschinenlesbaren Ausweise, wie z. B. des elektronischen Personalausweises ab 1.11.2010: Der Mikrochip ist kontaktlos auslesbar, d. h. die Daten können übermittelt werden, ohne dass man es merkt. Die entsprechenden Geräte dazu sind natürlich gesichert und werden nur an die zuständigen Behörden ausgegeben, aber auch hier ist kriminelle Energie denkbar.

Biometrische Daten
Heute definiert man Biometrie im Bereich der Personenerkennung auch als automatisierte Erkennung von Individuen, basierend auf ihren Verhaltens- und biologischen Charakteristika. Als biometrische Merkmale werden u.a. verwendet:

- Fingerabdruck (Fingerlinienbild),
- Gesichtsgeometrie,
- Handgeometrie,
- Handlinienstruktur,
- Iris (Regenbogenhaut),
- Körpergröße,
- Retina (Augenhintergrund) und
- Stimme.

2. Firmen als Datensammler

Kaum eine Anmeldung im Internet, in der man nicht Name, Vorname, Straße, Ort, Postleitzahl und E-Mail- Adresse angeben muss, und dies selbst bei einfachen Nachfragen zu einem Produkt, von Bestellungen ganz zu schweigen. Unbestritten benötigen die Firmen für „Rechtsgeschäfte“, so beim Online-Einkauf, die wahren Daten ihrer Kunden. Wohin sonst sollen sie die Ware schicken? Woher sonst sollen sie ihr Geld bekommen? Trotzdem mutet die Daten-Sammelwut selbst bei einfachen Anmeldungen mitunter erschreckend an, denn eigentlich würde bei vielen Anmeldungen nur ein Bruchteil der abgefragten Informationen genügen. Und dies sind nur die Fälle, in denen der Internetnutzer bewusst seine Daten angibt.

Personalisierte Werbung
Sie surfen im Internet auf der Suche nach Triathlon- Wettkämpfen? Und wundern sich, dass Sie auf dem Bildschirm bei verschiedenen Seiten plötzlich Werbung für Schwimmbrillen, Trinkflaschen und Laufschuhe bekommen? Sie wurden mit sehr ausgefeilten Methoden „gescannt“ und Ihr Internet- Surfverhalten protokolliert. Mitschuld daran sind sogenannte „Cookies“ (zu deutsch „Kekse“).

Apple. Google. Facebook. Amazon - Film der Landesanstalt für Medien Nordrhein-Westfalen (LfM)

Cookies sind (meist kleine) Datenpakete, die auf Ihrem Computer gespeichert werden: Im Gegensatz zu den vielen Tausend anderen kleinen Datenpaketen auf Ihrem Rechner werden sie automatisch angelegt und können von bestimmten Anbietern wieder ausgelesen werden. Anfänglich gab es nur eine Form von Cookies, die nunmehr als Browsercookies bezeichnet werden.

Browsercookies, auch http-Cookies genannt:

- werden vom Anbieter (einem „Server“) an den heimischen Computer („Client“ genannt) übertragen und dort gespeichert
- können vom Server wieder angefordert werden, wobei die Rücklieferung nur an den Ursprungsserver erfolgt
- Typische Einsatzgebiete sind: Warenkörbe bei Bestellsystemen; Anmeldeinformationen bei Webmailsystemen, bei Suchmaschinenanfragen, Wikis u. Ä.

In der Regel kann der Benutzer entscheiden, ob Cookies zugelassen werden. Aber es kann auch passieren, dass eine Internetseite ohne Cookies gar nicht funktioniert! An sich sind Cookies nicht direkt gefährlich, aber in ihnen können Daten, die der Profilbildung dienlich sind, gespeichert werden. In jedem Browser (wie Internet-Explorer oder Firefox) gibt es die Möglichkeit zu sehen, welche Cookies gespeichert sind und man kann diese auch löschen. Mit der Einstellung „Browserverlauf löschen“ (Internet Explorer) bzw. „Private Daten löschen“ (Firefox) kann man Cookies und einige andere Daten automatisch und vollständig löschen. Vielleicht lohnt die Einstellung, dass diese Daten automatisch beim Beenden des Browsers gelöscht werden!

Flash-Cookies – eine neue Generation Cookies Relativ neu sind sogenannte „Flash-Cookies“. Vielleicht haben Sie sich schon einmal darüber gewundert, dass trotz ihres Cookies-Löschens die Einstellungen für die Suche in YouTube erhalten blieb? Schuld daran sind Cookies, die unabhängig vom Browser im Adobe Flash Player gespeichert werden und auch nur dort löschbar sind. Sie müssen manuell oder per Software (Flash-Cookie-Killer, Flash-Cookie-Manager, CCleaner) gelöscht werden. Für den Browser Firefox gibt es dazu inzwischen eine Browsererweiterung „Better Privacy“ (unter https://addons.mozilla.org).
Die Speicherung dieser Datenkekse lässt sich auch mit dem Einstellungsmanager des Flash-Players konfigurieren, der allerdings nur online über die Adobe-Website zugänglich ist (Für Spezialisten: Unter Mac OS X oder Linux einfach dem entsprechenden Ordner die Schreibrechte entziehen.).

3. Soziale Netzwerke und der Datenschutz

In Bezug auf den Datenschutz stellen Netzwerke wie schülerVZ, wer-kennt-wen, Die Lokalisten, facebook u. v. a. natürlich besondere Herausforderungen dar, auf die in Kapitel 5 und in den Arbeitsblättern ausführlich eingegangen wird. Zunächst einmal ist es interessant zu wissen, was Betreiber Sozialer Netzwerke eigentlich dürfen, also welche Informationen sie speichern dürfen, welche weitergeben etc.

Werbung in Sozialen Netzwerken: Forderungen der Daten- und Verbraucherschützer
Die Daten- und Verbraucherschützer fordern für alle Netzwerke, dass jeder wählen können soll, ob er personalisierte, also auf seine Wünsche und Vorlieben zugeschnittene Werbung, allgemeine Werbung oder eben gar keine Werbung bekommen möchte, und das nur nach expliziter Zustimmung (Opt-In-Prinzip). Üblich ist bisher nämlich, dass derjenige, der nicht möchte, dass seine persönlichen Daten zu Werbezwecken ausgewertet werden, sich aus dem Werbesystem explizit abmelden muss (Opt-Out-Prinzip).
Generell gilt, und das ist nicht verwunderlich, dass die allgemeine Akzeptanz von Werbung auf Plattformen sehr hoch ist, solange die Mitgliedschaft nichts kostet. 37% der Nutzer befürworten laut der Studie „Soziale Netzwerke – Modeerscheinung oder nachhaltiges Geschäftsmodell?” der Wirtschaftsprüfungsgesellschaft PricewaterhouseCoopers eher die Einführung personalisierter Werbung als ein Gebührenmodell.

Richtlinien für Anbieter Sozialer Netzwerke
Bereits im April 2008 hatten die Obersten Aufsichtsbehörden für den Datenschutz in der Wirtschaft klare Leitlinien für die Betreiber von Sozialen Netzwerken und Bewertungsportalen im Internet formuliert. Hier einige Eckpunkte daraus:

- Anbieter Sozialer Netzwerke müssen ihre Nutzer umfassend gemäß den gesetzlichen Vorschriften über die Verarbeitung ihrer personenbezogenen Daten und ihre Wahl- und Gestaltungsmöglichkeiten unterrichten. Das betrifft auch Risiken für die Privatsphäre, die mit der Veröffentlichung von Daten in Nutzerprofilen verbunden sind. Darüber hinaus haben die Anbieter ihre Nutzer aufzuklären, wie diese mit personenbezogenen Daten Dritter zu verfahren haben (zu finden in den Datenschutzerklärungen der Sozialen Netzwerke!).
- Nach den Bestimmungen des Telemediengesetzes (TMG) ist eine Verwendung von personenbezogenen Nutzungsdaten für Werbezwecke nur zulässig, soweit die Betroffenen „wirksam darin eingewilligt haben“ (so die Formulierung, d. h. sie müssen der Nutzung bei der Anmeldung ausdrücklich zugestimmt haben).

Die vollständige Presseerklärung dazu unter: http://datenschutz-berlin.de. In die Suchmaske Soziale Netzwerke eingeben, dann die Pressemitteilung vom 22.04.08 auswählen.

Anbieter in der Pflicht – Umsetzung der Forderungen
Anfang 2009 unterzeichneten die Betreiber der reichweiten-stärksten deutschen Social Communities unter dem Dach der Freiwilligen Selbstkontrolle Multimedia-Diensteanbieter e.V. (FSM) eine konkrete Selbstverpflichtungserklärung zum Kinder- und Jugendschutz in den Angeboten schülerVZ, studiVZ, meinVZ (alle studiVZ Ltd.), lokalisten (Lokalisten Media GmbH) und wer-kennt-wen.de (lemonline media Ltd.).
(www.fsm.de/inhalt.doc/VK_Social_Networks.pdf)

Die Betreiber verpflichten sich, vor allem junge Nutzer durch technische Maßnahmen vor Missbrauchshandlungen Dritter wie beispielsweise Cyber-Mobbing zu schützen und durch eine verstärkte Aufklärung von Minderjährigen, Eltern und Pädagogen gezielt darauf hinzuweisen, welche Datenschutzmöglichkeiten bestehen. Konkret setzen die Unternehmen folgende Mechanismen ein:

- deutlich sichtbare Hinweise zum Schutz der Privatsphäre auf Informationsseiten direkt nach dem Registrierungsprozess
- standardmäßig voreingestellte strenge Privatsphäreneinstellungen bei unter 14-Jährigen
- optionale Sperrung der Auffindbarkeit der Profile durch Suchmaschinen
- keine Auffindbarkeit der Profile von unter 16-Jährigen durch externe Suchmaschinen sowie keine Möglichkeit der Aufhebung dieser Einstellung
- **Ignorierfunktion**: die Möglichkeit, andere Nutzer von der Community-internen Kommunikation zu sich selbst auszuschließen
- prominent platzierte Funktion zum Melden regelwidrigen Verhaltens und rechtswidriger Inhalte

Auch auf europäischer Ebene gibt es diese Form der Selbstverpflichtung der Anbieter. So unterzeichneten führende Betreiber, darunter studiVZ, facebook, Myspace, Google, Microsoft, Yahoo am Safer Internet Day am 10. Februar 2009 eine ähnliche Erklärung zum Jugend- und Datenschutz. (www.datenschutz.rlp.de/downloads/misc/sn_principles.pdf).

Praktische Umsetzung
Diese Anforderungen sind in der Praxis, vor allem was die Informationspflichten zur Datenverarbeitung und -weitergabe angeht, sowie die Formulierung in nutzerfreundlicher Sprache, nicht bei allen Anbietern Sozialer Netzwerke erfüllt, wie jüngst eine Abmahnung des Verbraucherzentrale Bundesverbandes zeigte.
Der Forderungskatalog der Verbraucherschützer:
www.vzbv.de
Weitere Infos zur Abmahnung der Verbraucherschützer:
www.vzbv.de

Neuen Kommentar schreiben