PRIVATSPHÄRE 3.0

Ein Plädoyer für einen bewussten Umgang mit persönlichen Daten im Zeitalter von Facebook, Google und Co.

Warum der selbstbestimmte Umgang mit persönlichen Daten im Web 2.0 wichtig ist.

Version 1.5

"Sie vertrauen mir, diese Idioten." - Mark Zuckerberg, Facebook Gründer

"Wenn Sie etwas machen, von dem Sie nicht wollen, dass es irgendwer erfährt – dann sollten Sie es vielleicht gar nicht erst tun." - Eric Schmidt, CEO Google

„Privatsphäre ist eine Illusion.“ - Larry Ellison, Chef von Oracle

„Du hast sowieso keine Privatsphäre, vergiss es einfach.“ - Scott Mc Nealy, Ehemaliger Chef von Sun Microsystems

Das sind Zitate wichtiger Persönlichkeiten von Internetfirmen mit denen viele von uns täglich zu tun haben. Das sollte uns nachdenklich stimmen!

Alles so schön bunt hier

Hast Du Dich schon einmal gefragt, womit Internetfirmen wie Facebook, Google oder Twitter Geld verdienen? Stellen sie dir ihre Dienste kostenlos zur Verfügung weil sie so nett sind? Sicher nicht! Vielmehr geht es darum personenbezogene Daten zu sammeln und diese an verschiedene Interessengruppen zu verkaufen. Nicht umsonst werden Facebook, Google und Twitter von Analysten hoch bewertet obwohl keine Gebühren von den Anwendern verlangt werden. Diese sowie andere Technologieanbieter, wie beispielsweise Oracle oder Apple werden nicht müde das Zeitalter der Post-Privacy auszurufen. Was sie damit meinen ist nichts anderes als die Abschaffung der Privatsphäre. Interessanterweise sind es gerade diese Firmen, die stark von der Datensammlung profitieren, da Sie die technische Infrastruktur anbieten oder Benutzerdaten verkaufen.

Leider sind die Mechanismen und Zusammenhänge im Internet für den normalen Benutzer wenig nachvollziehbar. Deshalb zieht die schöne Fassade in Form von sozialen Netzwerken und kostenlosen Apps und Onlinediensten immer mehr Benutzer an, die bereitwillig private Informationen über sich und andere preisgeben.

Nichts zu verbergen?

Typische Aussagen von Benutzern wie *"Ich habe doch nichts zu verbergen"*, *"Solange ich bei Facebook nichts schreibe, gebe ich nichts preis."* oder *"Das darf ruhig jeder wissen"* zeugen von einer weit verbreiteten Naivität im Umgang mit modernen Medien. Die technischen Möglichkeiten zur systematischen Ausbeutung umfassender persönlicher Informationen werden vielfach unterschätzt.
Grundsätzlich hat wohl jeder etwas zu verbergen. Die Frage ist nur vor wem. Oder würde es Dir gefallen wenn Dir bekannte und unbekannte wüssten wann und wie lange Deine Wohnung leersteht, wo Du gerne ißt, was Du gerne kaufst, welche Krankheiten und sexuelle Vorlieben Du hast, wer Deine Freunde sind und welche politische Gesinnung Du hast? Würde es Dir gefallen von anderen massiv manipuliert zu werden?

Das Internet vergisst nichts

Informationen die einmal im Internet sind bleiben dort für immer! Anders als wir Menschen vergisst das Internet nie etwas. Bei vielen Diensten stimmst Du mit der Veröffentlichung Deiner Daten der uneingeschränkten Nutzung durch den Dienstanbieter zu. Das bedeutet nichts anderes als das der Anbieter mit den Daten tun kann was er will. Bei Facebook räumst Du beispielsweise durch die allgemeinen Geschäftsbedingungen eine nicht-exklusive, übertragbare, unterlizensierbare, unentgeltliche, weltweite Lizenz zur Verwertung Deiner Daten ein. Veröffentlichte Daten werden nie gelöscht, sondern nur deaktiviert um die Integrität des Datenpools nicht zu verletzen. So kann es sein, das Informationen, die Du vor vielen Jahren im Internet veröffentlicht hast, morgen Deine Jobaussichten drastisch schmälern. Vielleicht wirst Du mit Deinem Profilbild auch ungewollt zum Werbeträger für ein Produkt für das Du einfach mal „Gefällt mir“ geklickt hast.

Wohin die Reise geht

Die langfristigen Schattenseiten sind wahrscheinlich wirtschaftliche Diskriminierung sowie Manipulation der freien Willensbildung und des individuellen Verhaltens. Wichtiger als das, was Du bekommst - Wen stört schon das bisschen Werbung? - ist das, was Du nicht bekommst. Beispielsweise der Immobilienkredit, die Berufsunfähigkeitsversicherung, den Job oder die Möglichkeit der freien Meinunsäußerung. Die Grenzen zwischen einfachen Werbeeinblendungen und gezielter Manipulation sind fließend. Ist es nicht gespenstisch wenn Dir Dein Handy fortwährend gute Vorschläge unterbreitet was Du als nächstes tun könntest und aufzeichnet, ob Du es auch wirklich tust? – Natürlich gesteuert von den Interessengruppen, die für Deine Daten bezahlt haben! Andere entscheiden, was Du siehst und was nicht. Du verlierst die Kontrolle. Die Visionen der Akteure in den verantwortlichen Unternehmen deuten darauf hin, dass sich die aktuelle Entwicklung des Internets eher zum Nachteil der Benutzer gestalten wird. Dabei wirst Du zum manipulierbaren Spielball der Interessen von Wirtschaft und Regierung. Durch gezielte Einflussnahme und gesteuerte Meinungsbildung wird Konformismus gefördert und Individualismus verhindert. Die Datenberge werden schon heute angehäuft. Bereits heute gibt es Organisationen, wie beispielsweise die Vengeful Librarians (schräger Name, was?), die gezielt Meinungsströme analysieren und versuchen Einfluß auf die Meinungsbildung auszuüben. Die Missbrauchspotentiale durch zukünftige „intelligente“ Technologien sind heute nur ansatzweise zu erkennen.

Was soll schon passieren?

Solange persönliche Daten isoliert bleiben sind die Missbrauchsmöglichkeiten relativ begrenzt. Anders sieht es aus wenn Daten zusammengeführt werden. Das passiert beispielsweise wenn Firmen Datenbestände verkaufen (oft Teil des Geschäftsmodells), Firmen komplett gekauft werden (Beispiel YouTube Übernahme durch Google in 2006), Daten gestohlen werden (Beispiel Sony Datenklau 2011), Benutzerkonten zusammengeführt werden (Änderung der Google Privacy Policy in 2012) oder Firmen von Regierungen zur Herausgabe verpflichtet werden (Beispiel US Partriot Act) und die Daten so ihren Besitzer wechseln. Daten die heute vielleicht noch sicher aufgehoben scheinen, können es morgen schon nicht mehr sein. De fakto Monopolisten, wie Beispielsweise Google oder Facebook verfügen bereits heute über eine hohe Konzentration persönlicher Daten. Wissen ist Macht! Folgende Szenarien sind in Zukunft durchaus realistisch:

- Produkte die mir angeboten werden sind immer teurer als die meiner Bekannten.
- Den Job habe ich nicht gekriegt obwohl ich doch super gepasst hätte.
- Die Versicherung hat meinen Antrag für eine Berufsunfähigkeitsversicherung abgelehnt.
- Angeblich bin ich nicht kreditwürdig. Auf Nachfrage sagt man mir der Computer gibt da so aus, da könne man nichts machen. Ich verstehe das nicht.
- Ständig bekomme ich passgenaue Werbung auf mein Handy. Ich kaufe oft Dinge, die ich nicht wirklich brauche.
- Während meiner Abwesenheit wurde bei mir eingebrochen. Woher wussten die, dass ich nicht Zuhause bin?
- Irgendjemand hat meine Identität übernommen und mein Konto geplündert.
- Jemand versucht mich und meine Kinder mit Fotomontagen zu diskreditieren.
- Seit die neue Partei die Mehrheit hat, werde ich ständig von Beamten bedrängt.
- Bürgerinitiativen werden zunehmend im Keim erstickt. Kritische Meinungen sind im Netz kaum noch zu finden.
- Opposition findet nicht mehr statt. Demokratisch ist das nicht.
- Meine Freunde im Land XYZ wurden verhaftet. Die Polizei fahndet auf Facebook gezielt nach Kritikern.
- Ich werde beschimpft, da ich einen Hund einer seltenen Rasse besitze.
- Regelmäßig werde gedrängt endlich dem sozialen Netzwerk XYZ beizutreten. Das machen ja schließlich alle so.
- Wieso bekomme ich neuerdings Medikamente gegen XYZ angeboten? Von meiner Krankheit habe ich doch nur meinem Arzt erzählt.

Ist es bereits zu spät?

Diese Entwicklung ist nicht abgeschlossen, sie steht vielmehr erst am Anfang. Viele Innovationen wie beispielsweise automatische Gesichtserkennung für Fotos oder Stimmungsanalyse und Manipulation in Online Communities sind in der Erprobung und werden bald auch Dich betreffen. Daher ist es wichtig sich nicht zu entziehen, sondern aktiv den Schutz der Privatsphäre einzufordern und durchzusetzen. Dies entspricht leider nicht dem aktuellen Zeitgeist, bei dem Privatsphäre als altmodisch gilt. Seitens der

Industrie und Regierung ist kaum Hilfe zu erwarten, da diese selbst zu den Profiteuren gehören. Da die Technologien unaufdringlich sind und vordergründig ausschließlich Nutzen bieten, bleiben Manipulationen größtenteils unbemerkt. Allerdings mehren sich glücklicherweise warnende Stimmen kritischer Journalisten und Informatiker.

Lesenswerte Hintergrundinformationen finden sich beispielsweise:

Die Datenfresser	http://datenfresser.info
Die Facebook-Falle	www.ixquick.com/do/meatasearch.pl?query=facebook-Falle+Sascha+Adamek
The Filter Bubble: What the Internet is Hiding from You (Untertitel in Deutsch)	http://www.thefilterbubble.com/ted-talk
Die Google-Falle	www.googlefalle.com
Initiative für mehr Privatheit	http://www.privat-im-internet.de/
Google Hintergrundinfos	http://www.kontrollausschluss.de/extra-der-meisterspion-google-und-seine-dienste.html#googlespionage

Wir, die Benutzer des Internets haben es in der Hand, wie weit wir die Aushöhlung unserer Privatsphäre zulassen wollen! Jeder kann handeln. Es kostet nichts und es ist einfach!

Tips zum Schutz der Privatsphäre im Internet

Damit Dir und Deinen wirklichen Freunden der Spaß in der Online-Welt nicht vergeht, kannst Du folgendes tun, um Deine Privatsphäre besser zu schützen und die Hoheit über Deine Daten zu behalten:

Tip 1:

Beteilige Dich nicht an an sozialen Netzwerken, sei ein NoBuddy. Beispielsweise Facebook analysiert und vermarktet Deine Daten im großen Stil und verfolgt fragwürdige Praktiken um die Grenze der Privatsphäre immer weiter zu verschieben. Wenn Du nicht auf ein soziales Netzwerk verzichten kannst, sei sehr sparsam mit persönlichen Informationen.

Tip 2:

Gebe in Foren und Communities keine echten Daten an. Beispielsweise für Geburtsdatum, Geschlecht, Telefonnummer etc. Ein hilfreicher Service gegen unliebsame Anrufer ist http://www.frank-geht-ran.de/.

Tip 3:

Publiziere keine persönlichen Informationen über Dich, Deine Familie und andere Personen im Internet. Auch über indirekte Informationen über andere lassen sich viele Erkenntnisse gewinnen.

Tip 4:

Verwende keine Email-Anbieter wie beispielsweise Google Mail oder Hotmail. Diese scannen und verarbeiten Inhalte Deiner Emails. Antworte möglichst nicht auf Emails dieser Absender, da auch die Antworten analysiert werden.

Tip 5:

Verwende eine sichere Suchmaschine. Beispielsweise Google verfolgt das Ziel personalisierte Benutzerprofile aus Deinen Suchanfragen zu erzeugen. Dies ist Teil des Geschäftsmodells. Alternativen sind www.ixquick.de oder www.startpage.com.

Tip 6:

Suche nicht über das im Browser eingebaute Suchfeld. Hierbei werden zusätzliche Daten zur Identifikation des Browsers an den Suchanbieter übermittelt.

Tip 7:

Verwende nicht den Browser Google Chrome. Chrome sendet umfangreiche Daten zur Auswertung an Google. Eine sichere Alternative, die auf dem gleichen Code basiert ist der Browser Iron www.srware.net/en/software_srware_iron_download.php. Google ist der Hauptsponsor von Firefox, so dass auch dieser Browser stark mit Google integriert ist.

Tip 8:

Erstelle kein Benutzerkonto bei Google (beispielsweise für Adwords oder iGoogle). Dadurch wird eine personenbezogene Auswertung deiner Online-Aktivitäten ermöglicht.

Tip 9:

Suche möglichst über eine verschlüsselte Verbindung (HTTPS) um den Zugriff von Internet Service Providern zu verhindern. Die Suchmaschine ixquick unterstützt dies.

Tip 10:

Verwende einen Browser, der über Merkmale zur Wahrung Deiner Privatsphäre verfügt. Beispielsweise Tracking Protection Listen oder InPrivate Browsing. Aktiviere diese Einstellungen. Beispielsweise Internet Explorer 9 (www.ie9.com) unterstützt diese Merkmale. Durch den Kommandozeilenparameter –private startet der Browser automatisch im InPrivate-Modus.

Tip 11:

Lösche alle Cookies nach jeder Browsersitzung. Die erschwert das Ausspähen von Verhaltensprofilen im Internet. Im InPrivate-Modus geschieht das automatisch.

Tip 12:

Schalte Geolocation bei neueren Browserversionen ab. Dies erschwert die Ermittlung Deines Aufenthaltsortes und die Erstellung von Bewegungsprofilen.

Tip 13:

Verwende nur anonyme Emailadressen und Pseudonyme für Foren und Internetdienste. Anonyme Emailadressen gibt es beispielsweise unter www.tempemail.net

Tip 14:

Verwende keine Smartphones bei denen unklar ist, welche Daten sie an die Provider übermitteln. Android Phones, iPhones und Windows 7 Phones zeichnen beispielsweise Bewegungsprofile auf, die von Apps und dem Provider ausgelesen werden können. Ein GPS Empfänger ist dafür nicht erforderlich. Smartphones wie beispielsweise das Apple iPhone oder Andriod-Smartphones bauen Tracking-Software wie beispielse Carrier IQ in das Betriebssystem ein, das in starkem Verdacht steht, regelmäßig persönliche Daten and die Hersteller zu übermitteln.

Tip 15:

Verwende keine Musikportale wie iTunes oder Zune für Musikdownloads. Diese analysieren Dein persönliches Medien-Konsumverhalten. Alternativ kann Musik im MP3-Format aus dem Internet bezogen und auf jedem MP3-Player abgespielt werden. Alternativ können CDs digitalisiert werden.

Tip 16:

Klicke nie auf Werbeanzeigen im Internet, da Deine Vorlieben dabei aufgezeichnet werden.

Tip 17:

Verwende keine Online-Festplatten oder Cloud-Dienste, da sich damit leicht Informationen über Dich ausspähen lassen. Alternativ kannst Du große USB-Sticks verwenden um Deine Daten transportabel zu halten.

Tip 18:

Widerspreche, wenn andere Fotos oder Informationen über Dich ins Internet stellen. Du hast ein Grundrecht auf informationelle Selbstbestimmung.

Tip 19:

Spreche mit Deinen Freunden und Kindern über Privatsphäre und diskutiere mögliche Konsequenzen. Sensibilisiere Dein persönliches Umfeld in Bezug auf informationelle Selbstbestimmung.

Tip 20:

Lasse Deine Addresse in Google Streetview und Bing Streetside anonymisieren.

Tip21:

Verschlüssle Emails mit sensiblem Inhalt. Beispielsweise mit PGP (http://de.wikipedia.org/wiki/Pretty_Good_Privacy).

STOP