Text: Simonne Baur

Digitale Selbstverteidigung

Digitale Überwachung ist allgegenwärtig

Überall hinterlassen wir digitale Spuren - ob im Netz, durch Smartphones oder sonstiger Verwendung von „smarten“ Geräten, beim Autofahren, via Kundenkarten, Bankkarten, E-Card etc.. Immer mehr Geräte sind heute mit Sensoren ausgestattet, mit dem Internet verbunden und ermöglichen so umfassende Einblicke in das Leben ihrer NutzerInnen. Gleichzeitig lassen sich mit automatisierten Methoden - Stichwort Big Data - schon aus rudimentären Metadaten über Kommunikations- und Online-Verhalten umfangreiche Persönlichkeitsprofile erstellen.
In einer Studie der Arbeiterkammer Wien wurde schon 2009 festgestellt, dass private und öffentliche Datenverwender in Österreich insgesamt bis zu 40 verschiedene Datenarten über eine einzelne Person speichern.
Quelle: AK Wien: „Privatsphäre 2.0. Beeinträchtigung der Privatsphäre in Österreich – neue Herausforderungen für den Datenschutz“, erschienen Februar 2009

Die Europäische Union arbeitet derzeit daran, eine Datenschutzgrundverordnung auf den Weg zu bringen. Erwünschtes Ziel wäre, dass Internet-Unternehmen ihren Nutzern zumindest eine Grundeinstellung zum Schutz der Daten liefern müssen, ohne dass der User selbst aktiv werden muss.

Es stellt sich die Frage, kann man sich überhaupt vor der digitalen Datenüberwachung schützen?

Fakten und Tipps zum Thema Computer und Umgang mit dem Internet

Prinzipiell gilt: Windows und MAC als Betriebssysteme sind wesentlich unsicherer als Systeme die auf Freier Software basieren, wie z.B. Linux. Die Fernsteuerung und das Ausspähen privater Daten kann sowohl durch sogenannte "Script Kiddies" (also Amateure, die mit im Internet verfügbaren Tools fremde Rechner angreifen können), als auch durch nationale und internationale Geheimdienste erfolgen.

Wie kann man sich schützen?

Durch den Einsatz von Proxy-Servern bzw. Virtual Private Networks (VPN) kann die Vorratsdatenspeicherung für den Bereich Internet weitestgehend umgangen werden. Dafür verbindet sich der eigene Rechner nicht mehr direkt mit der gewünschten Webseite, sondern baut eine verschlüsselte Verbindung zu einem Virtual Private Network auf, was dann wiederum erst die Webseite ansteuert. Durch die Verschlüsselung ist dem eigenen Internetanbieter nicht bekannt, welche Webseite aufgerufen wurde, und der Webseitenbetreiber findet nur die IP-Adresse des VPNs und nicht die des eigenen Anschlusses.

"Tor" – The Onion Router ist eine Software, die hilft, anonym im Internet zu surfen, ohne dass jemand herausfinden kann, welche Seiten man besucht. Dazu baut sie eine zufällig ausgewählte Verbindung zwischen mehreren Servern des Netzwerks in aller Welt auf. Tor ist damit ein Werkzeug zum Schutz der Privatsphäre oder auch ein Mittel, in autokratischen Regimen die Internetzensur zu umgehen.

Wie kompliziert ist Tor für den durchschnittlichen Internetnutzer?
Jacob Appelbaum: „Jeder, der einen Computer zu Hause hat, kann sich ein Programm namens Tor Browser Bundle herunterladen. Das klickt man an – und schon wird der zugehörige Browser durch das Tor-Netzwerk geleitet, ohne dass man irgendetwas konfigurieren muss. Und wer tiefer eintauchen will, kann es mit einem Instant Messenger nutzen oder damit E-Mails verschicken. Aber der erste Schritt ist: Es muss dir wichtig genug sein, dass du dich darum kümmerst.“ http://www.zeit.de/digital/datenschutz/2012-02/jacob-appelbaum-interview

Anleitung zur digitalen Selbstverteidigung:
https://netzpolitik.org/2015/digitale-selbstverteidigung-gegen-vorratsdatenspeicherung-wie-man-metadaten-vermeidet/

https://netzpolitik.org/2015/privacy-tools-anonym-surfen-mit-tor/

http://derstandard.at/2000024996193/Signal-Snowdens-Lieblingsapp-erscheint-fuer-Android?ref=rec

Google und Co wissen alles - unsere freiwillig hinterlassene Datenspur

„Ihre personenbezogenen Daten sind bei uns sicher und geschützt – und Sie behalten die Kontrolle darüber.“, das verspricht die meist genutzte Suchmaschine Google. Aber so gut wie überall sammeln Konzerne oder staatliche Organisationen detaillierte Daten von VerbraucherInnen, ob diese es nun wollen oder nicht. Im Sommer 2013 wurde durch den Whistleblower Edward Snowden bekannt, dass die National Security Agency (NSA) an E-Mail-Provider herangetreten war, um im großen Stil Kommunikationsdaten der Kunden anzufordern. Yahoo hat, wie andere Anbieter, im Nachlauf der Debatte über diesen Datenschutzskandal Transparenzberichte veröffentlicht. Die US-Behörden holten im ersten Halbjahr 2013 die meisten Daten von Yahoo-Kunden in den USA ein (12.444 Anfragen), gefolgt von Deutschland (4295) und in größerem Abstand von Italien, Taiwan, Frankreich und Großbritannien.

70 Prozent der Internetnutzer weltweit verwenden Google: 33 000 Suchanfragen pro Sekunde, 3 bis 4 Milliarden am Tag. Google durchsucht mehr als eine Billion Internetadressen.

Text: Simonne Baur

Was speichern Google, Facebook & Co.?

- Persönlichen Angaben, z. B. Name, Wohnort, Geburtstag, Kreditkartennummer.
- Aktivitäten: Postings, Kommentare, Fotos, Videos, Notizen, Aufenthaltsorte, Nachrichten und die Protokolle der letzten Chats und E-Mails. Selbst Veranstaltungen, zu denen Sie eingeladen wurden, sind gespeichert – ganz gleich, ob Sie zu- oder abgesagt oder gar nicht darauf reagiert haben! Genauso wie Reisebuchungen etc. Übrigens: Auch gelöschte Einträge bleiben gespeichert.
- Kontakte und Seiten – nicht nur aktuell bestehende Verbindungen, sondern auch gelöschte, dazu auch frühere, noch anhängige und sogar abgelehnte Anfragen von anderen Nutzern.
- E-Mail-Adressen – nicht nur selbst eingegebene, sondern auch automatisch zugeordnete aus Ihrem E-Mail-Konto oder dem Handy, wenn die mit Facebook abgeglichen (synchronisiert) wurden.
- Markierungen („Cookies“), die auf dem Computer hinterlassen werden, um zu erkennen, wenn Google, Facebook & Co. erneut vom selben Computer besucht werden.

Allein durch die Nutzung von Suchmaschinen werden Daten erfasst. Es empfiehlt sich dazu mal das „Kleingedruckte“ bei Google zu lesen:

„Daten, die wir aufgrund Ihrer Nutzung unserer Dienste erhalten: Wir erfassen Informationen über die von Ihnen genutzten Dienste und die Art Ihrer Nutzung beispielsweise dann, wenn Sie sich ein Video auf YouTube ansehen, eine Website besuchen, auf der unsere Werbedienste verwendet werden, oder wenn Sie unsere Werbung und unsere Inhalte ansehen und damit interagieren. Zu diesen Daten gehören:

- gerätebezogene Informationen

Wir erfassen gerätespezifische Informationen, beispielsweise das Modell der von Ihnen verwendeten Hardware, die Version des Betriebssystems, eindeutige Gerätekennungen und Informationen über das Mobilfunknetz einschließlich Ihrer Telefonnummer. Google verknüpft Ihre Gerätekennungen oder Telefonnummer gegebenenfalls mit Ihrem Google-Konto.

- Protokolldaten

Wenn Sie unsere Dienste nutzen oder von Google bereitgestellte Inhalte aufrufen, erfassen und speichern wir bestimmte Daten in Serverprotokollen. Diese Protokolle enthalten unter anderem Folgendes:

  - Einzelheiten zu der Art und Weise, wie Sie unsere Dienste genutzt haben, beispielsweise Ihre Suchanfragen.
  - Telefonieprotokollinformationen wie Ihre Telefonnummer, Anrufernummer, Weiterleitungsnummern, Datum und Uhrzeit von Anrufen, Dauer von Anrufen, SMS-Routing-Informationen und Art der Anrufe.
  - IP-Adresse.
  - Daten zu Geräteereignissen wie Abstürze, Systemaktivität, Hardware-Einstellungen, Browser-Typ, Browser-Sprache, Datum und Uhrzeit Ihrer Anfrage und Referral-URL.

- Cookies, über die Ihr Browser oder Ihr Google-Konto eindeutig identifiziert werden können.

◦ Standortbezogene Informationen

Wenn Sie Google-Dienste nutzen, erfassen und verarbeiten wir möglicherweise Informationen über Ihren tatsächlichen Standort. Wir verwenden zur Standortbestimmung verschiedene Technologien, wie IP-Adressen, GPS und andere Sensoren, die Google beispielsweise Informationen über nahe gelegene Geräte, WLAN-Zugangspunkte oder Mobilfunkmasten bereitstellen.

◦ Eindeutige Applikationsnummern

Bestimmte Dienste haben eine eindeutige Anwendungsnummer. Diese Nummer und installationsspezifische Daten, wie zum Beispiel Art des Betriebssystems oder Anwendungsnummer der Version, werden möglicherweise bei der Installation oder Deinstallation des entsprechenden Dienstes an Google gesendet oder wenn der Dienst zum Beispiel wegen automatischer Updates Kontakt mit unseren Servern aufnimmt.

◦ Lokale Speicherung

Möglicherweise erfassen und speichern wir Informationen (einschließlich personenbezogener Daten) lokal auf Ihrem Gerät, indem wir Mechanismen wie beispielsweise den Webspeicher Ihres Browsers (einschließlich HTML 5) und Anwendungsdaten-Caches nutzen.

◦ Cookies und ähnliche Technologien

Unsere Partner und wir verwenden verschiedene Technologien, um Daten zu erfassen und zu speichern, wenn Sie einen Google-Dienst aufrufen. Hierzu gehören möglicherweise auch Cookies oder ähnliche Technologien, mit denen Ihr Browser oder Ihr Gerät identifiziert wird. Darüber hinaus verwenden wir diese Technologien auch zur Erfassung und Speicherung von Daten, wenn Sie mit Diensten interagieren, die Teil unseres Angebots für Partner sind, zum Beispiel Werbedienste oder auf anderen Websites verfügbare Google-Funktionen. Unser Produkt Google Analytics unterstützt Unternehmen und Websiteinhaber bei der Analyse des Traffics zu ihren Websites und Apps. Bei Verwendung von Google Analytics zusammen mit unseren Werbediensten, z. B. solchen, die das DoubleClick-Cookie nutzen, werden Google Analytics-Daten vom Google Analytics-Kunden oder von Google mithilfe von Google-Technologie mit Daten über Besuche auf mehreren Websites verknüpft.“

Quelle: Auszug aus:
https://www.google.at/intl/de/policies/privacy/

„Die Intransparenz der Netzgiganten dient – wie die Geheimpolitik in Diktaturen – nur der Erhaltung ihrer Macht. Und deshalb bilden sie in ihrer Gesamtheit letztlich nichts anderes als ein autoritäres System”, warnt der rheinland-pfälzische Datenschutzbeauftragte Edgar Wagner.

Text: Simonne Baur

Quelle: http://www.bild.de/geld/wirtschaft/google/was-macht-google-mit-unseren-daten-35364024.bild.html

Gibt es Alternativen zu Google?

MetaGer ist eine deutsche Metasuchmaschine im Internet, die an der Universität Hannover als Dienst des Regionalen Rechenzentrums für Niedersachsen seit April 1996 entwickelt wurde. Seit 1. Oktober 2012 wird MetaGer vom eingetragenen Verein SUMA-EV in einer Kooperation mit der Universität Hannover betrieben und weiterentwickelt.
Die Datenübertragung von MetaGer erfolgt ausschließlich automatisch verschlüsselt über das HTTPS-Protokoll. Beim Betrieb von MetaGer werden keinerlei personenbezogene Daten gespeichert, weder Session-Cookies noch IP-Adressen und keine Browser-Fingerprints. Die IP-Adressen werden dabei bereits anonymisiert, während die Suche noch läuft, und sie werden von MetaGer nicht an die abgefragten Suchmaschinen weitergegeben. Auch die anonymisierten Adressen werden nicht gespeichert, da nicht auszuschließen ist, dass zukünftige Entschlüsselungsverfahren diese Daten deanonymisieren könnten. Es werden keine Nutzer-Profile angelegt, und es gibt keine Nutzerverfolgung ("User-Tracking"). Auch die Suchergebnisse von MetaGer können über einen anonymisierenden Proxy anonym erreicht werden - auch die dann weiterführenden Klicks. Weiterhin bietet MetaGer einen Zugang über das anonyme TOR-Netzwerk, den MetaGer-TOR-hidden Service. Die MetaGer-Server befinden sich ausschließlich in Deutschland und unterliegen dem im internationalen Vergleich strengen deutschen Datenschutzrecht.
Quelle: https://de.wikipedia.org/wiki/MetaGer

Ixquick ist eine aus den Niederlanden stammende Metasuchmaschine, die sich freiwillig verpflichtet, private Daten von Nutzern nicht zu erfassen oder zu speichern. Zur Verfügung steht auch eine geschützte Anfrage per TLS-Verbindung. Ixquick kombinierte ursprünglich diverse Suchmaschinen, einschließlich Google. Mit Stand Oktober 2015 werden nur noch Yahoo!, Gigablast und Yandex abgefragt.

Darüber hinaus wird unter dem Namen Startpage eine weitere Suchmaschine angeboten, die anonym ausschließlich auf Google zurückgreift. Ixquick hat seinen Sitz in den Niederlanden und New York und ein Teil der Server wird in den USA gehostet und unterliegt damit, wie alle Server in den USA, dem PATRIOT Act und ist verpflichtet, US-Behörden, wie dem FBI, der NSA oder der CIA ohne richterliche Anordnung den Zugriff auf die eigenen Server zu gewähren. Allerdings, da es sich um ein holländisches Unternehmen handelt, ist dieses vom in den USA bei Strafe bestehenden Schweigegesetz (nationale Sicherheit) nicht betroffen und kann den Zugriff veröffentlichen. Laut Ixquick werden Suchanfragen aus Europa aber grundsätzlich auf europäische Server gelenkt, es sei denn es kommt in Einzelfällen zu technischen Problemen. Außerdem gibt es seit 2014 eine neue Funktion in den Einstellungen, um für sich selbst den Serverstandort zu fixieren.
Quelle: https://de.wikipedia.org/wiki/Ixquick

Wenn ein Unternehmen allerdings seinen Hauptsitz in den USA hat, reicht es möglicherweise nicht, einfach ein paar Server in Europa aufzustellen, weil die US-Regierung der Meinung ist, auch darauf zugreifen zu dürfen.
Quelle: http://www.zeit.de/digital/datenschutz/2015-10/safe-harbor-eugh-konsequenzen/seite-2

Auf der Website von Ixquick findet man unterhalb der Suchergebnisse den Hinweis „In Partnerschaft mit Yahoo!, Yandex und hunderten mehr“. Diese übertriebene und irreführende Selbstdarstellung setzt sich im auf der Startseite geführten Slogan „Die diskreteste Suchmaschine der Welt“ fort, der weder belegt ist, noch dem direkten Vergleich mit auf Datenschutz spezialisierten Mitbewerbern wie Metager standhält.

Kann uns jemand durch die Webcam beobachten?

Fälle aus England und den USA zeigen, dass Geheimdienstbehörden im Zuge des Programms „Optic Nerve“ millionenfach Webcams aktiviert und auch völlig unbescholtene BürgerInnen auf diese unverschämte Weise überwacht haben. Allein in einem Zeitraum von sechs Monaten im Jahr 2008 soll der britische Geheimdienst GCHQ Bilder von 1,8 Millionen Yahoo-Nutzern eingesammelt haben. Darunter seien auch Aufnahmen sexueller Natur gewesen. Laut einem internen Wiki sei "Optic Nerve" auch 2012 noch aktiv gewesen.
Quelle: http://www.focus.de/politik/ausland/geheimdienst-im-schlafzimmer-briten-spionieren-millionen-webcams-aus_id_3648611.html

Wie kann ich mich schützen?

Am besten man klebt ganz einfach die Webcam zu und entfernt den Aufkleber nur, wenn man die Webcam selbst nutzt.

Fakten und Tipps zum Thema Datenschutz beim Handy

Text: Simonne Baur

Wie kann ich mein Handy schützen?

Jacob Appelbaum rät dazu, gar kein Mobiltelefon zu verwenden! „Oder wir müssen die Mobilfunktechnik so grundlegend neu entwickeln, dass sie keine Spionagetechnik mehr ist.“
Quelle: http://www.zeit.de/digital/datenschutz/2012-02/jacob-appelbaum-interview

Um die Menge an persönlichen Vorratsdaten zu verringern sollten eigentlich möglichst wenig „normale“ SMS geschickt oder „normale“ Telefongespräche geführt werden.
Eine ausführliche Info zur digitalen Selbstverteidigung ist hier zu finden:
https://netzpolitik.org/2015/digitale-selbstverteidigung-gegen-vorratsdatenspeicherung-wie-man-metadaten-vermeidet/

Kann auch der Text einer SMS ausspioniert werden?

Tatsächlich werden beim SMS-Verkehr nicht nur die Verbindungsdaten gespeichert, sondern auch die Inhalte. Bisher galt das nur für die zu Abrechnungs- oder Wartungszwecken üblichen sieben Tage - doch z.B. mit der neuen Speicherpflicht ist in Deutschland nun eine Zehn-Wochen-Frist vorgesehen.
Quelle: http://www.sueddeutsche.de/politik/vorratsdatenspeicherung-sms-inhalte-werden-gespeichert-1.2693495

Welche Nachrichten-App ist vertrauenswürdig?

Laut der Stiftung Warentest ist WhatsApp sehr kritisch zu beurteilen. WhatsApp setzt keine Ende-zu-Ende-Verschlüsselung ein, der Anbieter kann die Unterhaltungen zwischen den Chattenden also mitlesen. Sowohl die iOS- als auch die Android-Version übertragen Adressbucheinträge ohne Zustimmung des Nutzers oder der betroffenen Dritten. Zusätzlich teilen sie die Telefonnummer sogar Dritten mit – ebenfalls ohne Verschlüsselung. Die Android-Version sendet selbst Daten unverschlüsselt, die der Nutzer eingibt. Darunter könnten auch Gesprächsinhalte sein.

Die schweizer App Threema wird als eher unkritisch eingestuft. Threema ist für Android und iOS verfügbar und arbeitet mit einer Ende-zu-Ende-Verschlüsselung zwischen den miteinander Kommunizierenden. Auch der Anbieter selbst kann die Unterhaltungen also nicht verfolgen. Die iOS-Version sendet zwar die Nutzer-ID an Threema – dies ist jedoch notwendig und unkritisch, da die Informationen verschlüsselt werden. Die Android-Variante verzichtet vollständig auf die Übermittlung von Nutzerdaten an den Anbieter und Dritte. Beide Apps können die Adressbucheinträge speichern, allerdings nur in pseudonymisierter Form und mit ausdrücklicher Zustimmung des Nutzers. Die App ist auch verwendbar, wenn der Nutzer dem Auslesen seines Adressbuchs nicht zustimmt. Daten Dritter werden aus dem Adressbuch nach ausdrücklicher Zustimmung durch den Nutzer in pseudonymisierter Form an Server von Threema übertragen.
Eine Einschränkung des positiven Urteils gibt es jedoch: Threema ist keine quelloffene Software. Eine komplette Analyse des Datensendeverhaltens ist daher nicht möglich. Die Prüfer können

ausschließen, dass die App Nutzerdaten unverschlüsselt überträgt. Ob sie manche Daten aber eventuell verschlüsselt kommuniziert, konnten sie nicht zweifelsfrei feststellen.
Quelle: https://www.test.de/WhatsApp-und-Alternativen-Datenschutz-im-Test-4675013-0/?mc=kurzurl.messenger

Weitere Alternativen:
myENIGMA: Schweizer App, die einen sicher verschlüsselten Versand von Kurznachrichten und Multimediadateien bietet. Gruppenchats sind mit bis zu 30 Personen möglich (kostenlos für iOS, Android und Blackberry).

Telegram: Bietet „Geheime Chats“, in denen Nachrichten, Bilder und Videos verschlüsselt verschickt werden und sich nach Ablauf einer bestimmten Frist von selbst löschen (kostenlos für Android, iOS und Windows Phone)

Kik Messenger: Verlangt nicht wie WhatsApp die Handynummer des Nutzers/der Nutzerin. Mit den Kontakten können Inhalte jeglicher Art geteilt werden (kostenlos für Android, iOS und Windows Phone)

Sicher: Deutsche App, die sämtliche Daten verschlüsselt und darüber hinaus noch Passwortschutz, sich selbst zerstörende Nachrichten sowie Push-Mitteilungen ohne Vorschau bietet (kostenlos für Android, iOS und Windows Phone)

Signal: Open Source-Messenger, bei dem sämtliche Inhalte mit Ende-zu-Ende-Verschlüsselung übertragen werden (Textnachrichten, Bilder, Videos, Anrufe). Auch abhörsichere Telefonate sind möglich, wenn der Gesprächspartner ebenfalls Signal verwendet (kostenlos für Android und iOS; für Android hieß die App früher „TextSecure“).
Quelle: https://www.saferinternet.at/datenschutz/

Peilsender mit denen man auch telefonieren kann - Smartphones sind Spionagegeräte

Apple sammelt die Daten von Nutzern, das ist bekannt. Was aber viele vielleicht gar nicht wissen, in einem versteckten Bewegungsprofil in den Tiefen des iPhones werden auf einer Karte die Orte markiert, sowie Zeitpunkt und Dauer jedes Aufenthalts aufgezeichnet.

Zumindest gegen diese spezielle Art der Datensammlung von Apple kann man vorgehen.
Die Funktion kann im Menü „Datenschutz" deaktiviert werden, eine Anleitung dazu auf: http://www.gmx.at/magazine/digital/deaktivieren-standorterkennung-iphone-31152076

Bei diversen Navi-Apps kann „Location Tracking“ auch dann stattfinden, wenn die App nicht aktiviert ist. Dieses Tracking-Feature benötigt „die Sammlung, Verwendung und Öffentlichmachung der persönlichen Daten und der Darstellung der geographischen Daten wo man sich mit seinem Handy befindet.“
Quelle: http://media.arbeiterkammer.at/wien/PDF/NaviApps_2014.pdf

Text: Simonne Baur

Fakten und Tipps zum Thema Überwachung in sozialen Netzwerken

Im Zuge der Beantwortung einer parlamentarischen Anfrage im deutschen Bundestag wurden im November 2012 Pläne bekannt, wonach in Zukunft auch Chats und Postings in sozialen Netzwerken denselben Überwachungs- und Speicherregeln unterworfen werden sollen wie Telefonate. Demnach soll künftig auch gespeichert werden, wer mit wem wann und wo im Internet kommuniziert. Das Europäische Institut für Kommunikationsnormen (ETSI) arbeitet zu diesem Zweck an der kommenden Norm für eine Standard-Schnittstelle für „Lawful Interception" also „gesetzmäßige Überwachung", über die im Bedarfsfall auf die Inhalte der Kommunikation automatisiert und nahezu in Echtzeit zugegriffen werden kann.
Vorangetrieben wird das Projekt von den Innenministerien Frankreichs und Großbritanniens, wobei die britische Regierung hierzu bereits Anfang 2012 einen entsprechenden Entwurf zur „Communications Data Bill" vorlegte. An den Plänen beteiligt sich auch die Assoziation israelischer Elektronik- und Softwareindustrien, British Telecom, Vodafone, Siemens und eine auf Datenüberwachung spezialisierte Standardisierungsfirma namens Yanaa Technologies. Offiziell bestätigt wurde zudem, dass der Bundesverfassungsschutz Personal für die ETSI-Überwachungstruppe seit 2003 abstellt.
Quellen: https://de.wikipedia.org/wiki/Vorratsdatenspeicherung#Umgehungsm.C3.B6glichkeiten und http://fm4.orf.at/stories/1707197/

„Soziale Netzwerke" und die Freizügigkeit der Daten

Jacob Appelbaum sieht Facebook, das weltweit größte Soziale Netzwerk mit 1,44 Mrd. monatlich aktiven NutzerInnen (Stand: März 2015), als brisante Datenbank: „Benennen Sie einfach mal Facebook um in Stasibook. Wie gut fühlen Sie sich jetzt, wenn Sie dort Auskunft über die Aktivitäten Ihrer Freunde geben? Es ist furchteinflößend, wenn man sich vorstellt, dass wir uns alle gegenseitig überwachen. Wir haben den Stasistaat privatisiert und demokratisiert."
Quelle: http://www.zeit.de/digital/datenschutz/2012-02/jacob-appelbaum-interview

In Österreich nutzen rund 3,24 Millionen Menschen Facebook (August 2014)
Quelle: http://de.statista.com/statistik/daten/studie/296115/umfrage/facebook-nutzer-in-oesterreich/

Facebook führt regelmäßig Experimente mit NutzerInnen durch. Bei einer 2014 veröffentlichten und höchst umstrittenen Studie über Emotionen wurde das Verhalten von NutzerInnen nicht nur ohne deren Wissen untersucht, sondern es wurde dabei auch noch deren News-Feed manipuliert.
Quelle: http://media.arbeiterkammer.at/PDF/Digitale_Ueberwachung_im_Alltag.pdf S.23

Zum persönlichen Datenschutz auf Facebook finden sich hier einige gute Tipps:
https://www.datenschutz-hamburg.de/uploads/media/selbst_bewusst-Datenschutz_bei_Facebook_01.pdf

oder
saferinternet.at

Alternativen zu Facebook und Twitter

Unter dem Titel „How to Block the NSA From Your Friends List“ werden im Online Magazin Slate als Facebookalternative Diaspora oder Friendica und statt Twitter identi.ca empfohlen „Other projects, like Identi.ca (which is similar to Twitter), Diaspora, and Friendica are replacements for conventional social media networks, and they work. The number of users on federated networks is hard to calculate—again, their data are spread out instead of stored centrally—but Identi.ca alone counts 1.5 million users.“

Quelle:
http://www.slate.com/blogs/future_tense/2013/06/17/identi_ca_diaspora_and_friendica_are_more_secure_alternatives_to_facebook.html

Als Alternative zu Facebook ist auch das private Soziale Netzwerk ello zu erwähnen, wobei aber auch bezüglich des versprochenen Datenschutzes Kritik im Raum steht:
http://t3n.de/magazin/soziale-netzwerk-ello-zwischen-anspruch-wirklichkeit-237311/

Weitere Informationen zum Themenkomplex Überwachung gibt es in der November 2014 veröffentlichten Studie „Kommerzielle Digitale Überwachung im Alltag“ der Arbeiterkammer Wien:
http://media.arbeiterkammer.at/PDF/Digitale_Ueberwachung_im_Alltag.pdf