Fachhochschule Gelsenkirchen

if(is) internet-sicherheit.

Zum Tag des Datenschutzes 2011

Privatsphäre 2.0

Was braucht die Informations- und Wissensgesellschaft?

Positionspapier des Instituts für Internet-Sicherheit – if(is)

Stand: 25.01.11

Autor: Prof. Dr. (TU NN) Norbert Pohlmann
Institut für Internet-Sicherheit – if(is)
Fachhochschule Gelsenkirchen
Neidenburgerstr. 43
45877 Gelsenkirchen

Fon: 0209 / 9596 515
Handy: 0173 / 3021 838
E-Mail pohlmann@internet-sicherheit.de

1. Motivation

Die Bedeutung des Schutzes der informationellen Privatsphäre wird in der vernetzten Informations- und Wissensgesellschaft immer wichtiger. Durch das Internet werden zunehmend mehr personenbezogene Daten erzeugt, verarbeitet, weitergegeben und gespeichert.

Sowohl private Unternehmen als auch staatliche Stellen haben Interesse an personenbezogenen Daten.

Private Unternehmen wollen damit zum Beispiel Waren versenden, Rechnungen erstellen, aber auch zunehmend Kundenprofile generieren, die es ihnen ermöglichen, ein effektives Marketing zu entwickeln, Preise zu optimieren sowie die Zahlungsfähigkeit der Kunden besser einzuschätzen und Werbung verkaufen zu können.

Die staatlichen Stellen wollen in erster Linie die Verbrechensbekämpfung verbessern.

Ein immer größeres Problem ist der Internet-Nutzer selber. Er geht sorglos mit seinen persönlichen Daten um, es fehlen ihm der Überblick und das Verständnis für mögliche Probleme und den Verlust seiner Privatsphäre.

Privatsphäre

Privatsphäre bezeichnet den nicht-öffentlichen Bereich, in dem ein Mensch unbehelligt von äußeren Einflüssen sein Recht auf freie Entfaltung der Persönlichkeit wahrnimmt. Das Recht auf Privatsphäre gilt als Menschenrecht und ist in allen modernen Demokratien verankert. Dieses Recht kann aufgrund des öffentlichen Interesses an einer Person oder zu Zwecken der Strafverfolgung eingeschränkt werden [Wikipedia].

Informationelle Privatsphäre bedeutet also, dass jede Person das Recht hat, selber zu entscheiden, wem sie welche persönlichen Daten weitergibt. In Abhängigkeit, ob eine Person ihre persönlichen Daten an ihren Partner, Arbeitskollegen, Chef, Freunden, Sportkammeraden oder an die Allgemeinheit weitergibt, sind diese sehr unterschiedlich. Der Wunsch nach Privatsphäre kann in vielen Situationen unterschiedlich sein.

Wo liegen die Herausforderungen bei der informationellen Privatsphäre in unserer vernetzten Informations- und Wissensgesellschaft?

Woher bekommen die Internet-Unternehmen persönliche Daten der Nutzer?

Was muss der Nutzer tun, um seine Privatsphäre zu schützen?

Was müssen die Internet-Dienstanbieter tun, um die Privatsphäre ihrer Nutzer zu schützen?

Was sollte der Staat tun, um die Privatsphäre seiner Bürger zu schützen?

Klar ist, ohne einen angemessenen Schutz der Privatsphäre, wird das Internet an Bedeutung verlieren!

2. Wert der Privatsphäre

Die vernetzte Informations- und Wissensgesellschaft betrifft alle Branchen und Schichten. Es gibt in westlichen Gesellschaften niemanden, dessen persönliche Daten nicht in elektronischer Form vorlägen, gespeichert und übermittelt wurden – nicht nur Meldedaten und medizinische Daten, sondern auch persönliche Daten über verschiedenste Aktivitäten: Vereinsmitgliedschaft, Autokauf, Flugreise, Kontobewegungen, Einkauf, E-Mails, Google-Suche, Smartphone Nutzung und vieles mehr.

Im Leben jedes Menschen vergeht kaum ein Tag, an dem er nicht „elektronische Spuren" hinterlässt. Auch wenn diese nicht immer direkt etwas mit dem Internet zu tun haben, sind diese persönlichen Daten, wenn sie auf einem vernetzten Rechner liegen, im Prinzip dem Internet zugänglich und potentiell öffentlich. Entsprechend vervielfältigen sich auch die „elektronischen Spuren", so dass sich das Leben jedes Menschen sehr detailliert über elektronische Medien nachvollziehen lässt.

Die potentielle und reale Bedrohung, die von diesen gesammelten persönlichen Daten ausgeht, ist immens und vielfältig. Der Grund für das damit verbundene Angstgefühl liegt in der Bedeutung, die der Wert der Privatsphäre für uns Individuen, aber auch für die Gesellschaft besitzt.

Dennoch zeigt sich bei Nutzern mit einem positiven Grundvertrauen, dass sie nicht sensibilisiert genug sind, was den Umgang mit ihren persönlichen Daten angeht. Obwohl es im Internet keine absolute Sicherheit gibt, zeigen sie ein zu leichtfertiges Vertrauen. Die Nutzer fühlen sich aufgrund der Anonymität in der Masse sicher und geben sehr viel Persönliches von sich preis, besonders in Sozialen Netzwerken.

Es gibt durchaus Gesellschaften, in denen das Recht auf Privatsphäre bei weitem nicht den Stellenwert hat, wie in unserer. Historisch ist die Idee der Privatsphäre mit der Herausbildung der bürgerlichen Gesellschaft in politischer wie wirtschaftlicher Hinsicht verknüpft.

Eine Gesellschaft, die wirtschaftlich und politisch auf die Eigenverantwortlichkeit des Einzelnen setzt, muss umgekehrt das schützen, was den Einzelnen als Wirtschaftsfaktor und als Sozialwesen ausrüstet: einerseits seinen materiellen Besitz, andererseits seine persönliche Integrität.

Jeder marktwirtschaftliche Staat hat das Interesse, den Besitz von Wirtschaftsgütern – also auch Information als Wirtschaftsgut – zu schützen! Im Sinne der Verbrechensbekämpfung hingegen ist dem Staat an Möglichkeiten der Einblicknahme in persönliche Daten gelegen.

Dieser Unterschied zeigt sich etwa in den typischen Haltungen der unterschiedlichen Ministerien. Das Wirtschaftsministerium fordert alle Unternehmen auf, sich gegen Wirtschaftsspionage zu schützen. Das Innenministerium hat das Ziel, Verbrechen zu bekämpfen, bevor sie stattgefunden haben. Das betrifft die Terrorbekämpfung, aber auch andere kriminelle Handlungen wie z.B. Kinderpornografie, Amokläufe etc. Daher besteht der Wunsch, Vorratsspeicher anzulegen, das heißt, verdachtsunabhängige und längerfristige Zwangsspeicherungen der Kommunikationsdaten von Handy, Telefon und Internet – präventiv, um sie bei Bedarf abrufbar zu machen. Dieser Vorgang berührt die informationelle Selbstbestimmung, greift stark in die Privatsphäre ein und führt somit zu einem Vertrauensverlust in den Staat.

Auf der anderen Seite müssen wir feststellen, dass viele Internet-Dienstanbieter zunehmend weit mehr persönliche Daten ihrer Nutzer haben, als der Staat über die Vorratsspeicherung je erzielen wollte. Aber in diesem Bereich sind sehr viele Internet-Nutzer nicht informiert und interessenlos. Es fehlt den Internet-Nutzern das Bewusstsein und die Kenntnis über die Zusammenhänge, was für persönliche Daten über sie von den Dienstanbietern gespeichert

werden. Sie haben ihre persönlichen Daten den Unternehmen explizit oder implizit anvertraut und können deren weiteres Schicksal nicht mehr beeinflussen. Oft liegen diese persönlichen Daten im Ausland und unterliegen anderen Gesetzen. In der Regel sind sich Menschen ohne spezielle Sensibilisierung auch gar nicht bewusst, dass die Tatsache, dass sie einen Flug gebucht haben, im Prinzip von jedem Internet-Rechner der Welt aus nachvollzogen werden kann, wenn das Reisebüro, die Fluggesellschaft und der Flughafen nicht wirksame IT-Sicherheitsmaßnahmen ergriffen haben.

Egal, ob es um aktive oder um passive Nutzung von Informationstechnologie geht: Die Vorstellung einer totalen Offenlegung des Lebens des Menschen ist ein Schreckensszenario, dem wir entgegentreten müssen und auch können, ohne auf die Möglichkeiten der Informationstechnologie verzichten zu müssen.

3. Informationelle Selbstbestimmung

Das Recht auf informationelle Selbstbestimmung ist das Recht des Bürgers, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen. Daten sind personenbezogen, wenn sie eindeutig einer bestimmten natürlichen Person zugeordnet sind oder diese Zuordnung zumindest mittelbar erfolgen kann. Das informationelle Selbstbestimmungsrecht ist eine Ausprägung des allgemeinen Persönlichkeitsrechts und wurde vom Bundesverfassungsgericht im sogenannten Volkszählungsurteil vom 15. Dezember 1983 als Grundrecht anerkannt. Das informationelle Selbstbestimmungsrecht ist die Grundlage für das Bundesdatenschutzgesetz sowie die Landesdatenschutzgesetze und in einer Reihe von spezifischen Gesetzen geregelt.

Datenschutz steht für die Idee, dass jeder Mensch grundsätzlich selbst entscheiden kann, wem und in welchem Umfang seine persönlichen Daten zugänglich sein sollen. Der Datenschutz will den gläsernen Menschen verhindern und damit die Privatsphäre schützen!

Dazu sind im Datenschutz einige datenschutzrechtlichen Grundprinzipien festgelegt, wie z.B.:

- **Zweckbindung**
  Schutzziel, das gewährleisten soll, dass personenbezogene Daten, die zu einem bestimmten Zweck erhoben wurden, nicht für andere Zwecke verwendet werden dürfen, es sei denn, dass der Betroffene zugestimmt hat.
- **Erforderlichkeit**
  Rechtsbegriff, der zum Ausdruck bringt, dass Maßnahmen, die in die Rechte des Betroffenen eingreifen, voraussetzen, dass die Maßnahmen unabdingbar sein müssen, um einen bestimmten Zweck zu erreichen, und keine gleichermaßen wirksame Maßnahme zur Verfügung steht.
- **Datensparsamkeit / Datenvermeidung**
  Danach dürfen nicht mehr Informationen, als für den erstrebten Zweck erforderlich sind, über eine Person erhoben und verwendet werden. Hierzu gehört auch die Pflicht, von den Möglichkeiten der Anonymisierung (Anonymization) und Pseudonymisierung (Pseudonymization) Gebrauch zu machen.

4. Wie kommen Unternehmen an die persönlichen Daten ihrer Nutzer?

Die Frage, wie Unternehmen an persönlichen Daten ihrer Nutzer herankommen, ist sehr interessant und vielschichtig.

Erfassen von persönlichen Daten der Nutzer durch einen Dienstanbieter

Für die strukturierte Erfassung von persönlichen Daten eines Nutzers gibt es im Prinzip explizite und implizite Möglichkeiten für den Dienstanbieter.

Explizite Erfassung von persönlichen Daten

Bei der expliziten Erfassung von persönlichen Daten sind die Nutzer selbst aktiv und freiwillig beteiligt. Beispiele sind alle Angaben bei der Registrierung von Internet-Diensten, Feedback-Aktionen, Fragebögen, Umfragen, „I like" / „gefällt mir" Button, usw. Bei einer Registrierung gibt es z.B. einige Pflichtfelder die immer ausgefüllt werden müssen, damit der Dienst genutzt werden kann, aber auch freiwillige Felder, die nicht ausgefüllt werden müssen.

Implizite Erfassung von persönlichen Daten

Bei der impliziten Erfassung von persönlichen Daten ist der Nutzer nicht aktiv und bewusst nicht an der Datengenerierung- und Speicherung beteiligt. Beispiele für Techniken und Verfahren sind: Nutzen von Cookies, Anwenden von spezielle Toolbars, Auswerten von Browser-Historien, Nutzen von Maustracking-Verfahren, Auswerten von Webserver-Logfiles, Durchführen von E-Mail-Scanning, Positionsbestimmung durch das Auslesen von GPS-Infos, GSM-Koordinaten oder WLAN-Namen, usw.

Einstellung von persönlichen Daten durch den Nutzer selber (User Generated Content)

Bei Web 2.0 Anwendungen, dem Mitmach-Web, stellen die Nutzer selbst alle Informationen ein. Der Dienstanbieter stellt nur die Web-Plattform zur Verfügung.

Ein Beispiel für Web 2.0 Anwendungen sind Soziale Netzwerke, wie Facebook, StudiVZ, SchuelerVZ, MySpace, YouTube, Xing, LinkedIn, Twitter und Co., wo sich Nutzer aus verschiedenen Gesellschaftsgruppen auf verschiedene Arten kennenlernen und miteinander vernetzen können. Bei Sozialen Netzwerken legen die Nutzer selber Profilseiten mit ihren persönlichen Daten wie Werdegang, Freunde und Hobbys an. Weitere Web 2.0 Anwendungen sind Blogs, Wikis und Tauschseiten für Bilder oder Videos, bei denen auch persönliche Daten durch den Nutzer selbst eingestellt werden.

5. Was machen Unternehmen mit den persönlichen Daten ihrer Nutzer?

Soziale Netzwerke, wie Facebook, verdienen ihr Geld vor allem mit Werbung. Die Nutzer zahlen nichts für den Internet-Dienst, verraten aber massenhaft persönliche Daten über sich, für die der Betreiber sich die Rechte über die AGBs geben lässt. Mit diesen persönlichen Daten erstellt der Betreiber eines Soziale Netzwerkes Nutzerprofile, die für den Verkauf von Waren und Dienstleistungen interessant sind, weil sie passgenaue, individualisierte Werbung

ermöglichen. Diese zielgenaue Werbung lassen sich die Betreiber eines Soziale Netzwerkes durch das Schalten von individualisierten Anzeigen gut bezahlen.

Dieses **Prinzip „Bezahlen mit persönlichen Daten“** wird auch bei anderen Diensten, wie Suchmaschinen, E-Mail-Diensten, Nachrichten-Diensten, usw. angewendet.

Profilbildung der Nutzer

Mit den gesammelten persönlichen Daten ihrer Nutzer sind die Internet-Unternehmen in der Lage, mit Hilfe von Datenaggregation, Data-Mining, usw., Cluster über die Bedürfnisse der Kunden und Verhaltensvorhersagen zu erstellen. Diese Profilbildung hat zum Ziel, so viel wie möglich über den Nutzer in Erfahrung zu bringen, sein Verhalten und seine Bedürfnisse einzuschätzen und dieses Wissen für eigene Zwecke oder für den direkten oder indirekten Verkauf zu vermarkten. 2009 erwirtschaftete z.B. Google 97 % des Umsatzes in der Höhe von 24 Milliarden US-Dollar allein mit Werbung!

Beispiel: Google

Die Privatsphäre ist durch die Erhebung und Verknüpfung von verschiedenen persönlichen Daten z.B. allein durch Google massiv gefährdet. Würden beispielsweise viele Google-Dienste genutzt werden, dann wüsste Google

- wer man ist und wo man wohnt (*Buzz, Checkout, Gmail, Profiles* etc.)
- welche sozialen Kontakte man pflegt (*Buzz, Gmail, Orkut, Talk, Voice* etc.)
- wo man sich gerade aufhält (Ortung per GSM-Zelle, GPS oder WLAN bei Google’s mobilen Diensten wie *Latitude, Navigation* oder *Near me now*; potentiell aber auch bei allen anderen Endgeräten, die WLAN-Signale empfangen)
- wo man hin will (*Earth, Maps, Navigation* etc.)
- welche Termine man hat (*Kalender, Sync* etc.)
- welche Interessen man hat (diverse Suchdienste sowie weitere Dienste und Produkte wie *Analytics, Blogger.com, Buzz, Chrome, Gmail, Groups, iGoogle, Knol, YouTube* u.v.m.)
- wie die Bankverbindung von einem lautet (*Checkout*)
- wer die Partner bei eigenen Finanzgeschäften sind, was man kauft, wie viel man dafür ausgibt und wann diese Geschäfte abgewickelt werden (*Checkout*)
- welche und wie viele Aktien(-fonds) man besitzt und was man diesbezüglich für Transaktionen abwickelt (*Finance*)
- wie die eigene DNS aussieht und was für Krankheiten man hat oder hatte, einschließlich entsprechender Therapien (*Health*)
- wie man aussieht (*Buzz, Gmail, Picasa, Profiles* etc.)
- welche Daten man allgemein am eigenen Rechner verarbeitet (*Chrome OS* und weitere Cloud Computing-Angebote)
- usw.

In der Studie „Google - die zwei Seiten des mächtigen Internet-Konzerns“ werden die Strategien und Dienste von Google dargestellt sowie Gefahren aufgezeigt, die sich aus der Nutzung dieser Dienste ergeben. Infolgedessen werden zahlreiche Hinweise gegeben, was Internetnutzer tun können, um entsprechende Risiken zu minimieren. Siehe:

http://www.internet-sicherheit.de/fileadmin/docs/publikationen/2011/Google-StudieV2.0.pdf

6. Risiken und Auswirkungen von Profilbildungen

Für einen Teil der Internet-Nutzer sind die individuellen Werbeangebote, die mit Hilfe der Profilbildung angezeigt werden, ein positiver zusätzlicher Dienst. Sie fühlen ihre Privatsphäre nicht verletzt.

Andere Internet-Nutzer sehen dies genau anders und fühlen sich in ihrer Privatsphäre verletzt! Ein wichtiger zu beachtender Aspekt ist, dass sich der Internet-Nutzer zunehmend mit dem Druck zur Preisgabe von persönlichen Daten konfrontiert sieht, da er ansonsten nicht am gesellschaftlichen Geschehen teilnehmen kann, da zu viele wichtige Dienste nach dem Prinzip „Bezahlen mit persönlichen Daten“ arbeiten. Soziale Netzwerke z.B. bringen Nutzer aus verschiedenen Gesellschaftsgruppen zusammen und ermöglichen den Nutzern, sich darzustellen. Sie schaffen auch neue Wege, Demokratie und Bürgerbeteiligungen zu gestalten, was für die ganze Bevölkerung uneingeschränkt möglich sein sollte. Das Prinzip „Bezahlen mit persönlichen Daten“ ist bei zu vielen wichtigen Internet-Diensten schon etabliert und „zwingt“ somit viele Bürger diese zu nutzen!

Ein weiteres Risiko von Profilbildung ist die informationelle Diskriminierung, da die Nutzer nur noch von „ihrem“ erstellten Profil entsprechende Informationen angeboten bekommen, was eine enorme Einschränkung darstellt. Die Gefahr nicht mehr an alle Informationen heranzukommen ist sehr groß und muss verhindert werden.

7. Schutz der Privatsphäre

Damit wir den hohen Wert der Privatsphäre erhalten und die Entfaltung der Persönlichkeit der Menschen ermöglichen können, sollten die verschiedenen beteiligten Akteure ihre eigene Verantwortung kennen und die richtigen Maßnahmen zum Schutz der Privatsphäre umsetzen.

Politiker und der Staat müssen die Privatsphäre der Bürger nachhaltiger schützen

Der Staat muss Randbedingungen schaffen, die einem Internet-Nutzer ermöglichen, notwendige Internet-Dienste, wie Suchmaschinen, E-Mail, Nachrichten, Location Based Services, usw. zu nutzen, ohne auf seine Privatsphäre verzichten zu müssen.

Hier stellt sich insbesondere die Frage, inwieweit oder unter welchen Bedingungen Internet-Dienste zu tolerieren sind, bei denen nicht über das direkte Bezahlen des Dienstes, sondern über das Zulassen von Profilbildungen, den Anbietern das indirekte Geldverdienen ermöglicht werden soll. Eine besondere und notwendige Herausforderung ist das Finden und die Umsetzung einer angemessenen Lösung mit den Anbietern, um gemeinsam den Schutz der Privatsphäre zu gewährleisten.

Eine weitere und wichtige Herausforderung ist die Aufklärung der Bürger über die Risiken. Der Staat ist dafür verantwortlich, seine Bürger auf das gesellschaftliche Leben vorzubereiten und dazu gehört heute die positive Nutzung des Internets. Es darf auch nicht sein, dass hier durch eine fehlende Bildung der Internet-Kompetenz neue Barrieren und Benachteiligungen in unserer Gesellschaft geschaffen werden.

Da diese Veränderung unserer Gesellschaft zurzeit die Dimension einer gesellschaftlichen Revolution annimmt, sollten wir hier die nötige Sorgfalt und Nachhaltigkeit vom Staat einfordern, die zurzeit noch nicht zu erkennen sind.

Die Diskussion über Google-Street-View zeigt deutlich, dass nur ein kleines Randthema diskutiert wird, was leicht zu verstehen ist, und die eigentliche Herausforderung, bezüglich des Prinzips „Bezahlen mit persönlichen Daten“, vielen Menschen einfach noch gar nicht bewusst ist.

Internet-Dienstanbieter sollen mehr Verantwortung tragen und Transparenz schaffen

Die Internet-Dienstanbieter müssen sehr viel deutlicher darstellen, welche persönlichen Daten sie von ihren Nutzern erfassen und welche Rechte sie sich in den AGBs dafür einräumen. Eine Nutzerzustimmung muss in einer für den Nutzer klaren und verständlichen Sprache formuliert sein, damit der Nutzer sich frei entscheiden kann, und das bevor er den Dienst nutzt.

Die Internet-Dienstanbieter sollten den Nutzern immer auch die Möglichkeit einräumen, ihre eigenen persönlichen Daten und Profile einzusehen, die von ihnen gespeichert sind. Dies schafft Transparenz und Vertrauen.

Dem Nutzer sollte zukünftig immer auch die Möglichkeit gegeben werden, einen Dienst nicht nur durch „Bezahlen mit persönlichen Daten“, sondern auch mit Geld zu begleichen!

Die Bürger müssen bewusster mit den neuen Möglichkeiten umgehen

Die Bürger müssen sich mit den Möglichkeiten und Gefahren des Internets auseinander setzten, um ihre persönlichen Daten besser schützen zu können.

Der Internet-Nutzer kann durch die Nutzung von sicheren Browsern, das Löschen von Browser-Historie und Cookies, nur die Eingabe in Pflichtfeldern bei Registrierungen, Nichtteilnahme an Umfragen, Nicht-Nutzung von „I like“-Botton, usw. dafür sorgen, dass weniger persönliche Daten von ihm gesammelt werden können.

Insbesondere bei Sozialen Netzwerken muss der Nutzer sich genau überlegen, welche persönlichen Daten er welchen anderen Nutzern und der Allgemeinheit zur Verfügung stellen möchte.

Nur wenn ein Nutzer die Kompetenz besitzt, sich angemessen im Internet zu bewegen, kann er seine Privatsphäre nachhaltig schützen. Das ist in der realen Welt auch so!

Eine Handlungsvariante ist dabei, dass wir nur die Internet-Dienste nutzen, die unsere Privatsphäre angemessen schützen! Die Macht der Internet-Nutzer ist sehr groß, insbesondere wenn sie organsiert wird!