Die Internetfalle

Was wir online unbewusst über uns preisgeben und wie wir das WorldWideWeb für uns nutzen können

von
Thomas R. Köhler

1. Auflage

FAZ Buch 2010

Verlag C.H. Beck im Internet:
www.beck.de
ISBN 978 3 89981 230 5

Thomas R. Köhler

Die Internetfalle

Vorwort

Jeder Internetnutzer kennt die Situation: Man besucht zum wiederholten Mal eine Internetseite oder einen Onlineshop und wird persönlich begrüßt, manchmal sogar mit dem eigenen Namen. Vielleicht hat man in ebendiesem Shop einen iPod gekauft und findet es nun wirklich nützlich, das neueste Zubehör – von der Schutzhülle bis zum Ladekabel – direkt beim nächsten Besuch angeboten zu bekommen.

Positive Erinnerungen kommen da auf, etwa an den Besitzer des Zeitungskiosks um die Ecke, der – wenn ich seinen kleinen Laden betrat – bereits vor mir wusste, dass ich an einem Dienstag unbedingt die F.A.Z. haben muss – wegen des famosen Technik-Sonderteils. Genauso wusste er, dass mittwochs immer zusätzlich die Lokalzeitung mit dem Immobilienteil von mir gewünscht wird. Als Kunde fühlt man sich da respektiert und hochwillkommen.

Aber dieses heimelige „Tante-Emma"-Gefühl kann im Internet sehr schnell kippen.

Nehmen wir einmal an, Sie haben sich auf einer Fahrradwebsite ausgiebig nach einem neuen fahrbaren Untersatz umgesehen und nun verfolgt Sie Fahrradwerbung auf Ihrem Weg durchs World Wide Web. Ob Nachrichtenportal oder Hobby-Community: Überall wo Sie hinsurfen, prangt bereits die Werbung des von Ihnen betrachteten, aber nicht gekauften Produktes samt Link zum Shop. Woher wissen die, dass Sie ...?

Möglicherweise sind auch Sie dem aktuellen Hype um das Social Network „Facebook" gefolgt und haben sich gerade dort angemeldet und gewundert, wie passgenau die Personenvorschläge sind, von denen die Software behauptet, dass Sie diese kennen könnten. Sie sind zum allerersten Mal dort, und schon weiß Facebook, wer Sie sind und mit wem Sie Kontakt haben. Gespenstisch, finden Sie nicht?

Vielleicht ist alles aber noch viel schlimmer, und Ihnen geht es wie einer unglücklichen Bekannten des Autors. Diese musste kürzlich feststellen, dass sie es – ganz ohne ihr direktes Zutun – im Internet bereits zu einiger „Berühmtheit" gebracht hatte: Private Fotos von ihr, die sie selbst als „Jugendsünden" bezeichnet, waren auf diversen Websites und Social Networks aufgetaucht – immer verlinkt mit ihrem Namen. Gepostet ganz offensichtlich von einem verschmähten „Ex". Eine mehr als

unfreundliche Aktion mit langanhaltenden Auswirkungen. Zumal es gar nicht so einfach, wenn nicht gar unmöglich ist, derartige Inhalte wieder rückstandslos zu entfernen.

Sicher ist das letztgenannte Beispiel nicht alltäglich, aber beileibe kein Einzelfall. Leider. Das Internet und insbesondere das Social Web sind zu einer riesigen Sammel- und Verwertungsstelle von persönlichen Daten geworden, die wir unbewusst über uns preisgeben – ganz einfach, indem wir bestimmte Websites besuchen oder Beiträge hochladen, die teils aber auch von Dritten – ohne unser Zutun – gefüttert wird. Das Internet weiß manchmal mehr über uns, als uns lieb ist.

Wie geht man damit um? Dem Internet und den neuen Medien per „Stecker raus" den Rücken zukehren – wie es verschiedentlich propagiert wird – ist sicher keine Lösung. So fehlt jede Kontrolle, was über einen selbst geschrieben oder welche Fotos oder Videos mit Personenbezug eventuell von Dritten hochgeladen werden. Unerwünschte Rückwirkungen auf die „Offline-Welt" – etwa bei der nächsten Bewerbung um eine Arbeitsstelle oder einen neuen Auftrag – sind nicht ausgeschlossen.

Dieses Buch beschreibt einen anderen – vielversprechenderen – Weg: „Die Internetfalle" steht für den aktiven Umgang mit den Risiken und Nebenwirkungen des Internets und des Social Web. Nur wer die Zusammenhänge und Wirkungsmechanismen der neuen Onlinewelten versteht, kann die richtigen Entscheidungen treffen und die typischen „Internetfallen" vermeiden. Sich gegebenenfalls wehren gegen Datensammelwut, Identitätsdiebstahl und Online-Mobbing – technisch und unter Umständen auch juristisch.

Vor allen Dingen hilft der Blick hinter die Kulissen der Webwelt in diesem Buch dabei, die vielfältigen Chancen und Optionen, die im Social Web stecken, zu erkennen und für sich selbst zu nutzen – im Berufs- wie im Privatleben.

München Thomas R. Köhler

PS: Sämtliche im Buch genannten Links waren zur Drucklegung des Buches nach bestem Wissen und Gewissen recherchiert. Vorsorglich sei jedoch darauf hingewiesen, dass sich ebendiese Links in unseren schnelllebigen Zeiten genauso schnell auch wieder ändern können oder möglicherweise im Netz nicht mehr auffindbar sind.

1 Die Risiken im Überblick

Im vorherigen Kapitel ist es bereits angeklungen: Die Nutzung des Internets bringt Risiken und Nebenwirkungen mit sich. Dabei spielt das persönliche Verhalten eine maßgebliche Rolle. Leider ist die Realität nicht so einfach, dass die Orientierung an einer bestimmten Handlungsempfehlung ausreichend wäre, die wesentlichen Risiken auszuschließen. Selbst das Nicht-Partizipieren im Internet birgt wie erwähnt Risiken. Es gibt kein Entkommen, sondern nur die Möglichkeit, sich mit den Umständen zu arrangieren. Daher ist es nötig, die wesentlichen Wirkungsmechanismen zu kennen, um für sich selbst, für das eigene Leben – online wie offline – die richtigen Schlüsse ziehen zu können. Sehen wir uns diese also nun im Detail an. Punkt für Punkt.

Vorsicht „Datenverschmutzung"

Bei jeder Nutzung eines rechnerbasierten Systems entstehen Daten. Daten sind praktisch ein Neben- oder Abfallprodukt jeder Informationsverarbeitung, egal ob wir im Internet Bücher bestellen, die Payback-Karte an der Tankstelle vorlegen, die Kreditkarte im Restaurant benutzen oder auch nur den Motor eines neuzeitlichen Autos anlassen. Immer hinterlassen wir eine Spur an Daten. Das ist keine neue Erkenntnis und überrascht Sie als Leser sicher nicht im Geringsten.

Was sich in den vergangenen Jahren geändert hat, ist, dass immer größere Anteile unserer Kommunikation elektronisch abgebildet werden. Es hat vor Jahren mit E-Mail und SMS angefangen, die Entwicklung ging weiter mit allen möglichen Formen von Instant Messaging und findet einen (vorläufigen) Höhepunkt in der Kommunikation über soziale Netzwerke.

Hinzu kommt, dass es immer billiger wird, Daten zu speichern und zu verarbeiten. Man denke allein an E-Mail-Archivierung. Es ist aufwendiger zu entscheiden, was gelöscht werden kann und was relevant ist und aufgehoben werden muss, als alle damit in Zusammenhang stehenden Daten – ungeachtet von Relevanz und Notwendigkeit – dauerhaft zu speichern. Die Folge: Alles wird dauerhaft gespeichert. Auch und gerade im privaten Umfeld. Anbieter von Online-E-Mail-Diensten wie Hotmail und Yahoo Mail bieten Ihnen nicht selten Gigabytes oder gar „unbegrenzten" Speicherplatz für Ihre Mails an. Wer will da noch löschen …

Dies gilt natürlich nicht nur für E-Mails, sondern auch für alle anderen Daten, die mit *Ihren* Transaktionen oder *Ihren* Kommunikationsbeziehungen zu tun haben.

Das klingt abstrakt. Aber nehmen wir mal an, Sie gehen auf eine Geschäftsreise und fahren mit dem Auto zum Flughafen, fliegen dann zum Zielort und nehmen dort einen Mietwagen. Dabei entstehen (unter anderem) Daten:

- bei der Onlinebuchung von Flug und Mietwagen,
- bei der Erstellung des Parktickets im Flughafenparkhaus,
- beim Besuch der Airline-Lounge,
- beim Boarding zum Flug,
- beim Kauf einer Flasche Whiskey mit Kreditkarte/Vielfliegerkarte im „DutyFree"-Shop als Mitbringsel,
- bei Abholung, später dann auch beim Parken, Betanken und bei der Abrechnung des Mietwagens,
- beim Mobilfunkprovider für die Nutzung des Gerätes in verschiedenen Funkzellen des eigenen Netzes und gegebenenfalls bei einem Roaming-Partner in einem anderen Land,
- beim Versand einer Statusmeldung „bin jetzt in Stockholm" über Twitter,
- ...

Bei der Onlinebuchung von Flug und Mietwagen entstehen Daten – sowohl bei Fluggesellschaft und Mietwagenfirma als auch bei der Kreditkartenfirma, über die Sie Ihre Reisen abrechnen. Natürlich müssen die Beteiligten diese Daten von Ihnen erhalten, um ihren Teil der vertraglichen Vereinbarung (Flugtransport, Bereitstellung eines PKW und Abrechnung der Kosten auf bequemer monatlicher Basis) erbringen zu können.

Dies gilt in gleicher Weise für den Mobilfunkprovider und dessen internationalen Roamingpartner – auch diese brauchen die Daten für die Abrechnung.

Twitter braucht natürlich auch Ihre Dateneingabe für die Erbringung des Services.

In all diesen Fällen geht es um die Primärnutzung. Die Daten werden aus Nutzersicht zum eigentlichen Zweck (Bereitstellung der Services und damit einhergehende Abrechnung) verwendet.

Kritisch wird es dann bei der Zweitverwertung von Daten, etwa der Kundendaten Ihres Vielfliegerprofils. Ist die Vielfliegerkarte gleichzeitig noch eine Kreditkarte, über die Sie wesentliche Teile Ihrer Ausgaben

abwickeln, weiß die Fluggesellschaft nicht mehr nur, wohin Sie fliegen, sondern auch, dass Sie gerne Whiskey trinken (oder zumindest kaufen) und welche Restaurants Sie in Stockholm besuchen. Setzen wir voraus, dass man dort mit unseren Daten sorgsam entsprechend den deutschen Gesetzen umgeht, so bleiben zumindest Profile von Viel- oder Wenigfliegern übrig, für die sich sicher Werbekunden interessieren. Für Lufthansa, Air Berlin, Sixt oder Europcar ist Lufttransport oder Autovermietung das Geschäftsmodell – auch wenn Daten anfallen und man sich dort sicher Gedanken über die Verwendung macht. Sie sind und bleiben dort der Kunde. Nicht wenige der Unternehmen, die in unsere Transaktionsbeziehungen eingeschaltet sind, sehen sich zudem als datenzentrische Firmen, für die nicht nur die Transaktionsdaten relevant sind, sondern die vor allem interessiert daran sind, möglichst umfassend Daten zu erheben und zu verwerten.

Daten sind nicht nur ein Nebenprodukt von Transaktionen. Auch unsere Kommunikation und sozialen Interaktionen hinterlassen immer mehr „Datenschatten", im gleichen Maße, wie die Kommunikation von Angesicht zu Angesicht („Face to Face") von elektronischer Kommunikation ergänzt oder ersetzt wird. Bei Google, Yahoo, Facebook, Twitter und den meisten anderen ist das Geschäftsmodell eben nicht der Betrieb einer Plattform, sondern die Verwertung der Daten.

Anders als Sie vielleicht vermutet haben, sind Sie dort *nicht* der Kunde. Der Kunde dieser Unternehmen ist das werbetreibende Unternehmen, das Nutzerprofile erwirbt, oder vielleicht sogar eine Regierungsorganisation, die ganz spezielle Nutzerdaten kauft. Letzteres ist übrigens mehr als eine Vermutung: Eine „Preisliste" von Yahoo für die Erbringung derartiger Dienste für Regierungsstellen in den USA ist Ende 2009 auf der Enthüllungs-Website Cryptome.org aufgetaucht.

Noch einmal: Sie sind nicht der Kunde. Sie sind nur der Datenlieferant. Insbesondere die US-amerikanischen Unternehmen – und das ist nun mal ein Großteil der hier genannten Internetunternehmen – haben für unser Verständnis eine recht eigenwillige Auffassung von der Hoheit über die Daten. Demnach „gehören" die Daten dem Unternehmen, das diese sammelt. Oder wie der amerikanische Security-Guru Bruce Schneier (www.schneier.com/) es bei seinen öffentlichen Auftritten formuliert: „Google owns your E-Mail."

Oder noch anders gesagt: Wir sind nicht Kunden bei Google, sondern wir, das heißt unsere Daten, sind Googles Produkt (für deren Kunden in der Werbebranche)! Gleiches gilt für Facebook und alle anderen Anbieter von überwiegend „kostenlosen" Diensten. Man könnte auch feststellen: Wir zahlen mit unseren privaten Daten in einer Art laufendem Micropayment dafür. Kostenlos ist nur vermeintlich kostenlos.

Im Umkehrschluss heißt das aber auch, dass kostenpflichtige Dienste nicht notwendigerweise besser sind, wenn es um den Umgang mit unseren Daten geht. So oder so geben wir Kontrolle ab.

Und fragen Sie nicht nach dem Staat: Der Gesetzgeber ist nicht schnell genug. Die Gesetzeslage hinkt um Jahrzehnte hinter der Realität her. Die Datenschützer können zwar mahnen, aber wenig ausrichten.

Wollt Ihr die totale Überwachung?

Während „Überwachung" nach alter Väter Krimi Sitte früher noch bedeutete „folgen Sie diesem Wagen", kann die Datenspur, die wir heute hinterlassen, auch anders genutzt werden: „Folgen Sie *jedem* Wagen" wird möglich – aufgrund fehlender Ressourcen früher undenkbar.

Genauso wie die Debatte um den Zugriff auf Kommunikationsdaten bereits veraltet ist und die Aufforderung an die Strafverfolger oder den Geheimdienst nicht mehr lautet: „hören Sie diesen Anruf ab" oder „schneiden Sie diese E-Mail mit", sondern längst ersetzt worden ist durch „schneiden Sie jedes Telefonat/jede E-Mail mit" oder „was wurde vergangene Woche bei dieser oder jener Telefon-/E-Mail-Korrespondenz kommuniziert?".

Was glauben Sie, was passiert, wenn wir alle nun viel, viel mehr E-Mails schreiben, um die eigentlichen Absichten zu verschleiern, wie es manchmal von Experten vorgeschlagen wird? Richtig, der interessierte Geheimdienst oder die interessierte Behörde wird sich ein paar neue Computer oder Festplatten kaufen, mehr nicht.

Auch Zusammenhänge, die heute nicht relevant sind, können in Zukunft relevant werden. Lassen sich die Datenspuren dann verfolgen? Im Zweifel ja, da die komplexen IT-Systeme unserer Zeit in vielen Fällen nichts mehr vergessen – und das nicht nur aufgrund der Sammelwut der Betreiber, sondern da es schlicht billiger ist, alles aufzuheben, als gezielt zu löschen.

Ein weißer Fleck war bisher die Videoüberwachung. Trotz Versprechen diverser Hersteller von Sicherheitsequipment war es bisher nicht möglich, etwa Personen auf Videos zu erkennen oder auch nur Bildinhalte „durchsuchbar zu machen". Videoüberwachung ist deshalb im Regelfall eine manuelle Tätigkeit mit zweifelhaftem Erfolg. Wer kann schon nach acht Stunden „auf den Monitor Schauen" noch die entscheidenden Vorgänge identifizieren? So wird Videoüberwachung meistens erst nachträglich, nachdem etwas passiert ist, genutzt, um etwa anhand einer Videoaufzeichnung einen Tathergang zu klären.

Anders als Texte eignen sich Bilder und insbesondere Bewegtbilder eben nur bedingt für ein automatisches Durchsuchen. Bereits das Auffinden eines bestimmten Videos auf Youtube wird zur Glückssache, wenn man nicht die Begriffe des Titels beziehungsweise aus der Beschreibung kennt. Diese sind nämlich durchsuchbar.

Neue Ansätze der Videoüberwachung – wie sie etwa an der Universität von Kalifornien, Los Angeles verfolgt werden (www.technologyreview.com/computing/25439/?a=f) – schließen diese Lücke, indem sie automatisch Bildinhalte beschreiben und damit durchsuchbar machen. Dazu wird das Bild in einzelne Bildelemente zerlegt. Diese werden anhand einer Datenbank (www.imageparsing.com) identifiziert. Die Aktivität oder Inaktivität der einzelnen Bildelemente wird verfolgt und automatisch in Textform dokumentiert, etwa so: „weißer PKW fährt Richtung ..., roter PKW hält an Kreuzung ..." Damit wird das Material der Überwachungskamera durchsuchbar und auswertbar.

Denkt man noch etwas weiter in die Zukunft und geht davon aus, dass sich bereits heute Kfz-Kennzeichen und zukünftig vielleicht auch Gesichter automatisch erkennen lassen, so ergibt sich – bei Vernetzung hinreichend vieler „dokumentationsfähiger" Kameras – tatsächlich ein Szenario, das einer vollständigen Überwachung nahekommt. Die von verschiedenen Aufsichtsbehörden eingesetzten Kennzeichenscanner, deren zivile Version bereits in vielen Parkhäusern zu finden ist, sind hier nur der Vorgeschmack.

Das Internet vergisst nichts

Technische Systeme vergessen nichts mehr. Wie oben bereits angedeutet, spielen die Kosten für Datenerfassung, Speicherung und vor allem für die Auswertung keine Rolle mehr. Die Frage ist, wie das mit unseren bisherigen Kommunikationsgewohnheiten harmoniert.

Was im persönlichen Gespräch oder am Telefon gesagt wird, ist begrenzt auf ein oder wenige Gegenüber. Eine breite Öffentlichkeit ist schon rein akustisch ausgeschlossen. Selbst wenn der Dialog im Mittelpunkt eines antiken Amphitheaters geführt wird, können kaum mehr als einige hundert Personen mithören. Eine Aufzeichnung und Veröffentlichung des geführten Dialogs kann dies bereits ändern. Solange dieses Dokument in einem Archiv verschwindet oder im Privatbesitz verbleibt, ist dies ebenfalls unproblematisch. Kompromittierenden Inhalt vorausgesetzt, kann diese vielleicht für eine Erpressung dienen, einer weiteren Öffentlichkeit bleibt der Inhalt jedoch im Regelfall verborgen.

Man kann durchaus die Auffassung vertreten, dass ein erheblicher Teil der Privatsphäre dieser „Alten Welt“ sich aus Ineffizienzen in der Technologie der Aufzeichnung und Verwertung ergeben, die es eben gerade nicht möglich machen, alles zu speichern und auffindbar zu machen.

Mit zunehmend internetbasierter Kommunikation verändern sich nun die Spielregeln: durch die Digitalisierung – also einfache Speicherungs- und Vervielfältigungsmöglichkeit – und die einfache Auffindbarkeit einzelner digitaler Inhalte mittels Suchmaschinen. Letztere beschränkt sich derzeit zwar weitgehend noch auf Textinhalte, funktioniert hierbei aber bereits erstaunlich gründlich.

Der Satz „das Internet vergisst nichts“, klingt daher wie eine Plattitüde. Und doch können Inhalte, etwa Äußerungen in verschiedenen Foren, oft genug noch jahrelang aufgefunden werden, selbst wenn der eigentliche Websiteanbieter seine Seiten zwischenzeitlich vollständig umgestaltet hat. Möglich machen dies Langzeit-Archivier-Funktionen von Suchmaschinen wie der „Google Cache“ oder Dienste wie www.archive.org. Auf letztgenannter Website lassen sich beispielsweise Webseiten, die der Autor mit seiner früheren Firma entwickelt hat, in allen möglichen alten Versionen in Text und Bild wieder hervorkramen – auch etwa der Stand von 1997 (!).

Ganz offiziell arbeitet auch die US-amerikanische Library of Congress an der dauerhaften Aufbewahrung digitaler Inhalte (www.digitalpreservation.gov). Die Library of Congress ist das Gegenstück zu den Nationalbibliotheken in Deutschland (www.d-nb.de), Österreich (www.onb.ac.at) und der Schweiz (www.nb.admin.ch) und archiviert alle Bücher, die jemals in dem Land erschienen sind. Zunehmend entdecken die Nationalbibliotheken aber auch die Archivierung digitaler Inhalte als Aufgabenfeld. Bei der Library of Congress bezieht sich die Arbeit an der sogenannten „digital preservation“ inzwischen auch auf scheinbare Trivialitäten, wie die Speicherung aller jemals über Twitter versendeten Kurznachrichten. Diese auch als „Tweets“ bezeichneten Botschaften mit maximal 140 Zeichen werden durch Übernahme des Archivs des Dienstanbieters rückwirkend seit dem Start des Dienstes in Jahr 2006 gespeichert und sind dauerhaft zugreifbar. Von Vergessen keine Spur.

Inoffiziell, aber wirksam ist auch die Website Wikileaks (www.wikileaks.org). Wie andere ähnlichen Seiten dient diese als Veröffentlichungsplattform für Dokumente, die Regierungen oder Unternehmen lieber unter Verschluss gehalten hätten.

Ich weiß, wohin Du gestern gesurft bist

Was kann, was darf ein Websiteanbieter über Sie wissen? Wenn Sie sich beim Webangebot persönlich mit Ihrem echten Namen anmelden, natürlich eine ganze Menge. Aber was ist mit dem Fall, dass sie einfach nur – ohne jede Anmeldung – eine Website besuchen?

Was Ihr Browser über Sie verrät

Grundlegende Informationen über die Systemumgebung Ihres Rechners werden bei jedem Websitebesuch übertragen. Ein Auszug des Systems, auf dem dieses Buch entstanden ist, liest sich dann in etwa so:

IP: XXX.XXX.XXX.XXX (unkenntlich gemacht)
Browser: Opera 9.80
OS: Windows XP
Herkunft: Germany
Bildschirmauflösung 1280x800
Cookies aktiviert
Javascript aktiviert
32bit Farbtiefe

Diese Angaben helfen der Website, die sie besuchen, dabei, die eigenen Inhalte so aufzubereiten, dass diese auf Ihrem Rechner optimal dargestellt werden können. Persönliche Informationen werden dabei nicht übertragen.

Aus der IP-Adresse (die hier unkenntlich gemacht wurde), lassen sich außerdem grundlegende Hinweise zur Herkunft ziehen. Bei Internetanschlüssen mit sogenannten „festen" IP-Adressen, wie sie im Regelfall von größeren Unternehmen verwendet werden, lässt sich immerhin eingrenzen, dass diese oder jene Abfrage aus dem Unternehmen „XYZ" kam. Bei privaten Nutzern und kleinen Unternehmen werden üblicherweise variable IP-Adressen, die sich bei jeder Einwahl beziehungsweise mindestens einmal in 24 Stunden ändern, verwendet. Aus diesen Adressen kann man Rückschlüsse auf den Provider und die geografische Region des Anschlusses ziehen. Übrigens auch ein Grund, weswegen man beim Internetsurfen gelegentlich auf Werbung für regionale Unternehmen stößt oder international auf Websites ab und an keinen Zugriff auf Inhalte erhält. Aus Anbietersicht bezeichnet man die Nutzung derartiger Auswertungen als „Regional Targeting".

Ihr Webbrowser verrät darüber hinaus recht wenig. Lediglich in der ersten Variante des Chrome Browser von Google gab es eine eindeutige Browser-Kennnummer, die die Identifikation eines jeden Browsers – unabhängig etwa von dem im folgenden Abschnitt diskutierten Cookies – ermöglicht. Nach Nutzerprotesten wurde dieses „Feature" aber wieder entfernt.

Die Wahrheit über Cookies

Insbesondere bei Internetneueinsteigern kreist die Diskussion über Internetrisiken häufig um die Gefahren oder vermeintlichen Gefahren der sogenannten „Cookies". Aber was ist damit wirklich gemeint, wenn von „Keksen" die Rede ist? Ein deutsches Wort für die hier angesprochene Bedeutung des Begriffs „Cookies" gibt es schlicht nicht.

Grundlegend ist das, was zumeist als „Browser-Cookie" oder „http-Cookie" bezeichnet wird, nichts anderes als eine Textdatei, die ein Webserver auf dem Rechner des Internetsurfers ablegen kann.

Bei späteren Besuchen der gleichen Website kann der Nutzer damit wiedererkannt werden. Diese Funktion ist für sich betrachtet nicht problematisch, sondern ein wesentliches Leistungsmerkmal aller aktuellen Webbrowser. Als solche ist sie auch standardisiert in den als „RFC" (Request for Comment) bezeichneten Internetstandards (RFC2109). Konkret bedeutet das: Präferenzen und Einstellungen des Nutzers können abgespeichert werden – ein Komfortgewinn für den Anwender (z.B. Anzahl Suchergebnisse pro Seite, Spracheinstellungen).

Für den Anwender beinhaltet das die Wiedererkennbarkeit eines Nutzers, sowohl während einer sogenannten Nutzersitzung (auch: Session) – etwa während eines Bestellvorgangs beim Onlineshopping – als auch bei einem wiederkehrenden Besuch des Nutzers auf derselben Website.

Unter Umständen ist über Cookies auch die Nachverfolgung (das Tracking) von Nutzern über verschiedene Sessions und Websites hinweg möglich und damit die Erstellung von Profilen über das Surfverhalten eines Nutzers. Dieser letztgenannten Möglichkeiten bedienen sich häufig Werbenetzwerke, aber auch Werkzeuge für die Reichweiten- und Zugriffsmessung im Internet.

Grundlegend betrachtet gibt es folgende unterschiedliche Arten von Cookies:

- *Session Cookies:* Diese haben nur eine kurze Lebensdauer. Sie werden gelöscht, sobald der Browser geschlossen wird.

- *Persistente Cookies* sind Cookies mit langer Lebenszeit, die eine länger dauernde Protokollierung des Surfverhaltens von Nutzern ermöglichen und wiederkehrende Nutzer auf einer Website erkennen können (wobei Erkennen sich auf das Wiedererkennen des Browsers bezieht, persönliche Daten zum Anwender liegen damit zunächst nicht oder noch nicht vor).

Zudem gilt eine Einschränkung: Cookies sind immer auf den Browser bezogen. Nutzt ein Anwender mehrere Browser, liefert das genauso „verfälschte" Ergebnisse wie bei der Nutzung eines Rechners und Browsers durch mehrere Personen (etwa im Familienkreis).

Aus Sicht dieses Buches besonders interessant sind Cookies von Drittanbietern (sogenannte „Third Party Cookies"). Denn unter Umständen ist es bei einem Website-Besuch möglich, dass auch Drittanbieter Cookies setzen. Eingebundene Werbebanner oder andere Elemente von anderen Websites wie sogenannte „Web Bugs" erlauben das Tracking des Nutzers auch über verschiedene Websites hinweg.

„Web Bugs" werden typischerweise von Anbietern von Webstatistik-Funktionen verwendet und bieten nicht nur Zählfunktionen für Besucher und Sessions auf der jeweiligen Website, sondern erlauben auch das Datensammeln über verschiedene Websites hinweg, die alle den gleichen Statistikservice benutzen. Die Firefox-Erweiterung „Cyberghost" gibt einen guten Überblick über die Trackingsysteme einer jeden besuchten Website und erlaubt auch selektives Blockieren einzelner Dienste.

Grundsätzlich gilt: Nur der Anbieter, der einen Cookie gesetzt hat, darf diesen auch wieder auslesen.

Session Cookies sind wegen der obengenannten Einschränkungen, vor allem hinsichtlich der Lebensdauer, als harmlos einzustufen. Persistente Cookies eignen sich für langfristiges Verfolgen von Websitebesuchen. Der Betreiber einer Suchmaschine kann damit (mit obengenannten Einschränkungen bei von mehreren Personen genutzten Rechnern) über die Laufzeit des Cookies verfolgen, welche Suchbegriffe abgerufen und welche Suchtreffer angeklickt wurden.

Trickreicher sind (persistente) Cookies von Drittanbietern, da diese sich dafür eignen, die Webbewegungen der Besucher langfristig über verschiedene Websites hinweg nachzuvollziehen. Der Anbieter erfährt damit große Teile der Internethistorie und weiß genau, wohin Sie tags zuvor gesurft sind.

Noch ist ein auf diese Weise ermitteltes Profil anonym. Erst die Eingabe der eigenen Daten (Name, Adresse ...) auf einer verbundenen Website, zum Beispiel einer Shoppingwebsite, die ebenfalls der Kontrolle des

Anbieters unterliegt, ermöglicht die Verknüpfung eines Profils mit einer Person.

Grundlegend verbieten zwar die meisten Datenschutzgesetze das Zusammenbringen von Personendaten mit Profildaten, nicht selten werden jedoch Fälle bekannt, in denen Anbieter derartiger „Services“ aus Drittländern heraus operieren und sich den deutschen Gesetzen damit entziehen.

Ein erster Selbstschutz ist über die Browsereinstellungen möglich. Die meisten gängigen Browser erlauben folgende Einstellungen und Aktionen zum Umgang mit Cookies:

- Keine Cookies annehmen.
- Keine Cookies von Drittanbietern annehmen.
- Vor dem Akzeptieren von Cookies nachfragen.
- Cookies beim Schließen des Browsers löschen.
- Inhalt des Cookies ansehen.

Abbildung 14: Cookie-Liste

Auch lassen sich Cookies – wie in der Abbildung am Beispiel des Firefox-Browsers zu sehen – anzeigen und gezielt löschen, so dass man einzelne, als nützlich empfundene Cookies behalten kann. Nützlich können diese etwa sein, um sich automatisch auf seiner Lieblings-Website einloggen zu können, ohne jedes Mal Nutzername und Passwort eingeben zu müssen.

Wie viele Nutzer tatsächlich von der Funktion Gebrauch machen, ist weithin unbekannt, auch wenn es einzelne Studien dazu gibt. Das Marktforschungsunternehmen Comscore geht von rund 30 Prozent der untersuchten Nutzer aus (nur US – siehe: www.drweb.de/magazin/flash-cookies-tricksen-cookie-loscher-aus/). Damit sind nur die klassischen Browser-Cookies gemeint.

Mit der weiten Verbreitung von Adobe „Flash“ – einer Browsererweiterung zum Anzeigen von Multimediainhalten und Filmen im Internet – kommt jedoch eine neue Art von Cookies hinzu, die permanent auf dem Nutzerrechner gespeichert wird und ein Wiedererkennen dessen erlaubt. Das Problem dabei: Flash-Cookies lassen sich nicht über die gerade genannten Funktionen des Webbrowsers verwalten und gegebenenfalls löschen, sondern nur mit Adobe Flash selbst (oder einem geeigneten Zusatzprogramm oder durch manuelle Suche in den Anwendungsdaten des Flash Players auf der eigenen Festplatte).

Abbildung 15: Flash-Einstellungsmanager

Den meisten Nutzern sind diese relativ neuen Verwandten der klassischen Cookies nicht bekannt. Aus Serversicht lassen sich die Funktionen von HTML und Flash-Cookie durchaus ergänzend einsetzen.

Das Fazit hier: Cookies sind größtenteils harmlos, aber nicht frei von Risiken.

Der Online-Fingerabdruck

Cookies sind nicht die einzige Möglichkeit für Anbieter, auf einen einzelnen Benutzer einer Internetanwendung zurückzuschließen. Auch die oben bereits genannten grundlegenden Eigenschaften des Webbrowsers können dazu bereits ausreichend sein.

Ob Internet Explorer, Firefox, Safari oder Chrome – jeder Browser kann so individuell konfiguriert sein, dass Website-Betreiber einen Nutzer wiedererkennen können. Die US-Bürgerrechtsbewegung Electronic Frontier Foundation (EFF) führt das nun mit dem vor kurzem veröffentlichten Tool Panopticlick (panopticlick.eff.org) vor.

Die Website zeigt an, welche Daten über das eigene System vorliegen und ob diese in Kombination hinreichend individuell sind, um einen Nutzer zu identifizieren.

Ein frisch heruntergeladener Browser ist grundlegend erst einmal nur über eine Versionsnummer erkennbar und damit stets einer von vielen gleichartigen. Zusammen mit dem Betriebssystem wird die Kombination schon seltener. Im Falle des Testrechners (Opera Browser auf Windows XP), der sich wie folgt meldet: „Opera/9.80 (Windows NT 5.1; U; de) Presto/2.5.24 Version/10.53“ ist nur noch ein System von 660 mit genau dieser Konfiguration online.

Zeitzone, Länderkennung und vor allem installierte Browsererweiterungen (sogenannte Plugins), aber auch im System vorhandene Schriften und die Bildschirmauflösung (hier 1400x1050 mit 32bit Farbtiefe) helfen in Kombination, eine Art „Fingerabdruck“ des Browsers zu erzeugen und damit eine Eindeutigkeit eines Systems im Testfall unter rund 1 Millionen Systemen zu belegen – ganz ohne den Einsatz von Cookies.

Browserhistorie einmal anders

Eine relativ neue Möglichkeit, als Anbieter mehr über den Nutzer zu erfahren, ist das indirekte Auslesen der Browserhistorie. Jeder Browser speichert – wenn man es als Anwender in den Systemeinstellungen nicht anders definiert – die besuchten Websites ab. Damit wird unter anderem erkennbar, welche in eine Webseite eingebundenen Links bereits besucht wurden. Dies wird farblich in der Darstellung hervorgehoben und wechselt in den meisten Fällen von blau zu hellblau.

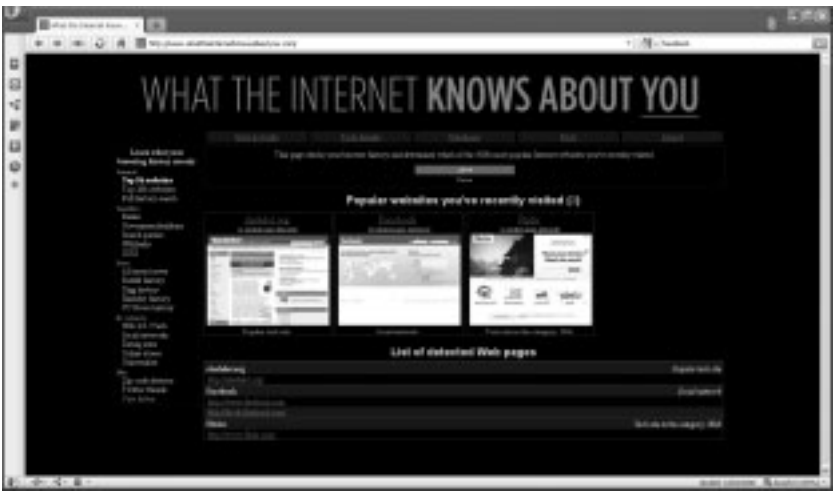

Abbildung 16: What the Internet knows about you

Durch geschickte Programmierung kann man nun als Anbieter von Websites alle möglichen Websites abfragen, ob diese bereits besucht wurden, und so in kurzer Zeit ein Bild von der Surfhistorie des jeweiligen Systems gewinnen. Die nachfolgende Abbildung zeigt auf deutliche Weise, was damit möglich ist.

Die Website „Whattheinternetknowsaboutyou.com“ ist eine recht allgemeine Demo. Weitere Anwendungen können auch gezielt eingesetzt werden. Der Treuetest (www.date-seiten.de/treuetest.html) zeigt etwa dem Lebens(abschnitts)-partner, ob sich der PC-Nutzer auf Dating-Websites herumgetrieben hat, während „Did you watch porn“ (didyouwatchporn.com) sich – nicht ganz ernsthaft – der Frage widmet, ob der Anwender pornografische Websites besucht hat.

Wer wie der Autor abstinent geblieben ist, wird sogleich mit einem friedlichen Häschenbild belohnt und konsequenterweise aufgefordert, nun endlich mal Entsprechendes anzusehen.

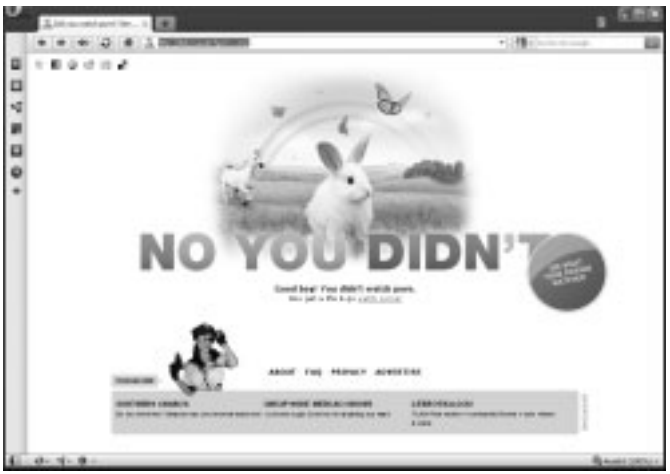

Abbildung 17: Did you watch ...

Zudem lässt sich die Website auch an Bekannte empfehlen. Klickt der per Facebook oder einen anderen Social-Media-Dienst Eingeladene dann auf die Seite, erfährt auch der Einladende etwas über die Präferenzen in dieser Richtung. Fazit: Eine originelle Anwendung, die aber wohl im wesentlichen Werbung verkaufen und Adressen sammeln soll. Vorsicht ist angebracht!

Ich weiß, wohin Du morgen surfen wirst

Suchmaschinen finanzieren sich durch Werbeanzeigen? Das stimmt nur bedingt. Mit dem, was Sie bei Google, Bing oder einer anderen Suchmaschine eingeben, sind Sie anonym? Allerdings stimmt auch das nur bedingt. Suchanbieter identifizieren wiederkehrende Benutzer nicht nur per IP-Adresse (die sich bei privaten Internetanschlüssen mindestens einmal täglich ändert) oder Cookies, sondern speichern auch die verwendeten Suchbegriffe und die aufgerufenen Ergebnisse. Anhand der Daten versuchen sie unter anderem auch zu erschließen, was der Nutzer in Zukunft suchen wird.

Google speichert nach Unternehmensangaben diese Suchen für 18 Monate und anonymisiert sie dann. Andere Anbieter speichern die Daten unter Umständen zeitlich unbegrenzt oder geben diese an Dritte weiter – mit unklarem Verbleib.

In gewisser Weise „bezahlen" Sie den Nutzen einer Suchmaschine nicht nur durch einen Austausch mit der Werbeeinblendung, sondern auch stets mit der Preisgabe von persönlichen Daten.

Verwenden Sie mehrere Dienstangebote bei einem Anbieter, bei dem Sie auch Websuchen benutzen – bei Google mit seinem Universum an Diensten mehr als naheliegend –, so vervollständigt sich das Bild, das der Anbieter vom Anwender bekommt. Eine De-Anonymisierung ist plötzlich kein Problem mehr. Nicht nur der Internetserviceprovider, der eine Zuordnung zwischen IP-Adresse und Anschlussinhaber eines Internetanschlusses (und damit vermutlich auch den Nutzer oder zumindest dessen Umfeld) herstellt, sieht damit Klartext.

Natürlich gehen wir alle grundlegend davon aus, dass wir dem Anbieter vertrauen können. Aber was, wenn die Daten in die falschen Hände geraten? Dies lässt sich nicht rückgängig machen. Die New York Times berichtet bereits am 9.8.2006 von einem Vorfall bei AOL, bei dem die gesammelten Suchdaten von 657.000 AOL-Nutzern öffentlich wurden – samt Informationen, die eine Identifizierung einzelner Nutzer erlauben. Bereits das Speichern der Suchanfragen ist damit potentiell gefährlich, da stets das Risiko des Abfließens der Daten an Dritte besteht.

Ich weiß, wo Du wohnst

Trauen Sie Ihrem Internetprovider? Vermutlich mehr als Ihrem Suchanbieter oder einem anderen Websitebetreiber.

Vermutlich sind Sie davon überzeugt, dass Ihr Zugangslieferant Ihre Daten nicht anders als zur Rechnungsstellung und zur Erfüllung seiner gesetzlichen Pflichten, etwa im Rahmen der Vorratsdatenspeicherung, verwendet.

Als Bürger Großbritanniens können Sie (beziehungsweise konnten Sie) zumindest zeitweise andere Erfahrungen machen. Ohne Vorwarnung wurde etwa bei British Telecom (BT) – der ehemalige Telefon-Monopolist in UK (von der Marktstellung vergleichbar mit der Deutschen Telekom hierzulande) – ein Großversuch mit Kunden vorgenommen, bei dem ein Internetwerbesystem einer Firma „Phorm" zum Einsatz kam.

Der Werbeanbieter nutzt hierbei Daten, die er direkt vom Provider erhält, um mittels Paketinspektion („deep packet inspection") das Surfverhalten der Nutzer im Internet zu analysieren und passende Werbung bereitzustellen. Die IP-Pakete für Port 80 bekommt Phorm nach Unternehmensangaben in anonymisierter Form von den ISPs geliefert. Im Gegenzug teilt Phorm die durch den Verkauf von Werbeflächen erzielten Einnahmen mit den Internetprovidern.

Dadurch, dass der Internetverkehr durch Phorm umgeleitet wird, sieht Phorm nicht nur die aufgerufenen Seiten, sondern auch die Seiteninhalte und alle Eingaben, die auf den Sites gemacht werden, und kann Cookies unter dem Namen anderer Websites setzen. Klingt kompliziert und ist es auch – eine detailliertere Beschreibung für technisch Interessierte findet sich hier: www.theregister.co.uk/2008/02/29/phorm_documents/ und auf der Website von Securityforscher Richard Clayton (www.cl.cam.ac.uk/~rnc1/080518-phorm.pdf).

Nicht alle Angaben von Phorm lassen sich demnach überprüfen, insbesondere gilt dies für die Angabe von Phorm, dass die Daten anonym sind. Problem dabei: Die Anonymisierungsfunktion wird auf den Rechnern, die von Phorm beim Serviceprovider installiert werden, betrieben und von Phorm auch gewartet und verwaltet. Würden Sie Phorm vertrauen?

Zweifel sind erlaubt, wenn man die Historie des Unternehmens näher kennenlernt:

Gegründet wurde die Firma Phorm von einem Herrn, dem die britische Presse Beziehungen (www.thisismoney.co.uk/markets/article.html?in_article_id=430955) zum russischen Geheimdienst nachsagt und der derselben Quelle zufolge bereits in der Vergangenheit – mit der Vor-

läuferfirma „People on Page“ Software, die von verschiedenen Security-Firmen als Spyware bezeichnet wurde, entwickelt hat (zur Einstufung siehe F-Secure: www.f-secure.com/sw-desc/peopleonpage.shtml).

Diese Aufzählung liefert durchweg Anlass für Skepsis. Die Bedenken werden noch größer, wenn man das Verhalten der Serviceprovider betrachtet: Vorgesehen war, bei BT und anderen Internetserviceprovidern die Nutzer mehr oder weniger zwangsweise einzubeziehen. Nur „Opt-Out“ wäre möglich, das heißt ein aktiver Widerspruch des Nutzers würde zum Ausschluss vom Programm führen, alle anderen Nutzer des Internetzugangs beim jeweiligen Anbieter wären automatisch dabei.

Auch wenn BT nach eigenen Angaben inzwischen von dem System Abstand genommen hat, lässt der harte Preiswettbewerb unter den Internetzugangsanbietern erwarten, dass auch zukünftig – bei BT und anderswo – Wege gesucht werden, aus den Nutzerdaten Kapital zu schlagen. Für die Provider ist die Sache klar: Endlich können Sie vom immer größer werdenden Onlinewerbekuchen, den sie bisher Google und Co überlassen mussten, selbst partizipieren.

Einen ähnlichen Weg wie Phorm, aber für das mobile Internet, nutzt etwa der Provider Orange auf Basis eines Systems der vom Mobilfunkausrüster Qualcomm übernommenen irischen Startup-Werbefirma „Xiam“ (Quelle: www.theregister.co.uk/2008/03/12/mobile_phom/). Kurz gesagt, überträgt das System die Phorm-Idee auf mobile Plattformen und nutzt vom Provider bereitgestellte Daten, wie etwa die Chronik der aufgerufenen Seiten und Rechnungsdaten für die Bereitstellung individualisierter Werbung.

„Xiam“ und „Phorm“ sind die Pioniere in einer Welt, in der Provider gerade damit beginnen, die Vielzahl von Daten, die sie durch die Bereitstellung ihrer Dienste ganz automatisch sammeln, zu Geld zu machen. In Deutschland, Österreich und der Schweiz wurde bisher kein Einsatz von Phorm oder Xiam bekannt.

Ich weiß, wo Du bist

Wenn Sie an Ihr eigenes Leben denken: Wer wüsste besser über Sie Bescheid als Ihr Mobilfunkprovider? Oder gehören Sie zu den wenigen, die ihr Telefon nicht immer mit sich tragen? Aus Sicht eines Forschers sind die Vielzahl der Daten, die bei Mobiltelefonnutzung anfallen, ein hochinteressantes Forschungsgebiet, aus Sicht des Mobilfunkproviders eine noch zu erschließende Goldmine. Die Rede ist dabei von sogenannten „Call Detail Records“ (kurz CDR), den Verbindungsdaten. Ein

CDR entsteht für jede Sprach- oder Datenverbindung. Er beinhaltet – unter anderem – für Sprachverbindungen die Ursprungs- und Zielrufnummer, die Art und Dauer der Verbindung und natürlich auch die ID des Mobilfunkmasten, über den das Endgerät den Anruf weitergereicht hat. Damit lässt sich der ungefähre Standort berechnen.

In Summe können CDRs auch ermitteln, wie weit dieser eine bestimmte Telefonnutzer innerhalb eines Zeitraums, also zum Beispiel eines Tages, gereist ist, welche Orte er dabei besucht hat oder wo er (vermutlich) wohnt oder arbeitet. Vergleicht man die Daten mit den Daten von Verkehrsmitteln und -wegen, so lässt sich auch festhalten, ob jemand mit dem Flugzeug, der Bahn, dem Fahrrad oder dem Auto verreist ist und ob er mit dem Auto gegebenenfalls gar zu schnell gefahren ist. Natürlich reden wir derzeit nur von anonymer Auswertung, Ihr Führerschein ist also (derzeit) noch nicht in direkter Gefahr.

Forscher des US-Telekommunikationsunternehmens AT&T haben so herausgefunden (www.technologyreview.com/communications/25396), dass etwa Leute in Manhattan durchschnittlich 2,5 Meilen pendeln, während Vergleichszahlen aus Los Angeles auf weitere Strecken hindeuten (in der Untersuchung waren es rund 5 Meilen). Bisher keine weltbewegenden Erkenntnisse, aber die Forschung steht hier erst am Anfang.

In der Tat können derartige Daten in aggregierter Form sehr nützlich sein, etwa für die Planung von Haltestellen für den ÖPNV oder zur Ermittlung von Staus auf Autobahnen und Bundesstraßen. Hierzu arbeitet etwa der Navigationssystemhersteller TomTom mit Vodafone zusammen und ermittelt aus (anonymisierten) Echtzeitbewegungsdaten von einer Vielzahl von Mobiltelefonen auf definierten Strecken (Autobahnen/Bundesstraßen) Stockungen und Staus und teilt sie allen Besitzern entsprechender Endgeräte mit – in vielen Fällen schneller und zuverlässiger als der herkömmliche Verkehrsfunk.

Gelingt es jedoch, die Mobilfunkdaten zu de-anonymisieren, so lassen sich auch Szenarien finden, die für den Nutzer wenig erfreulich sind, etwa das bereits angedeutete als indirekte Überwachung der gefahrenen Geschwindigkeit – automatischer Strafzettel inklusive.

Jeder Fernsehkrimiseher weiß, dass auch für die Aufklärung von Verbrechen Bewegungsdaten von Mobiltelefonen herangezogen werden, auch wenn, anders als im Krimi suggeriert, ein „Anruf beim Provider“ dafür – zumindest bislang – nicht ausreicht.

Ich weiß, wer Du bist

Wer könnte besser Bescheid wissen, als ein Anbieter, dem die Kunden Kontaktdaten, private Fotos und Nachrichten an Freunde und Bekannte anvertrauen? Stellvertretend für die Gattung der Netzwerke steht hier Facebook, der Social-Web-Dienst mit der größten Nutzerzahl.

Was Facebook über Nutzer weiß

Facebook ist wie ein guter Freund, der nichts für sich behalten kann. Kein Anbieter ist derzeit auch nur annähernd so groß und so bedeutsam. Bei keinem Anbieter ist die „Stickiness" so hoch. Von „Stickiness" (Klebrigkeit) spricht man in der Fachwelt bei einer Website, wenn Nutzungsdauer und Wiederbesuchshäufigkeit hoch sind. Hier hat Facebook durch die Verlagerung weiter Teile der privaten Kommunikation weg von anderen Diensten in sein eigenes System und die Einbindung fremder Websites durch Öffnen seiner Schnittstellen für viele Nutzer fast so etwas wie ein paralleles Internet geschaffen und dadurch eine sehr hohe Stickiness. Gleichzeitig erhält Facebook durch die Nutzerinteraktionen eine Fülle an Daten über jede einzelne Aktivität jedes einzelnen Nutzers – und damit Informationen über die Interessen von mehr als einer halben Milliarde Menschen weltweit.

Gleichzeitig steht kein anderes Web-2.0-Unternehmen derzeit so in der Kritik wie Facebook. Dabei galt es bei seinem Start durchaus als Musterknabe in Sachen Wahrung der Privatsphäre seiner Nutzer. Wie sehr sich Facebook in dieser Hinsicht gewandelt hat, hat die Electronic Frontier Foundation (EFF) mit Bezug auf das jeweilige Jahr zusammengefasst (www.eff.org/deeplinks/2010/04/facebook-timeline, Übersetzung durch den Autor):

Facebook Privacy Policy 2005:

Keinerlei persönliche Informationen stehen Nutzern dieser Website zur Verfügung, die nicht zu mindestens einer Gruppe, die in Deinen „Privacy Settings" definiert sind, gehören.

Facebook Privacy Policy 2006:

Wir verstehen, dass Du es nicht möchtest, dass jeder in der Welt Zugriff auf die Informationen hat, die Du auf Facebook teilst. Daher geben wir Dir Kontrolle über Deine Informationen. Unsere Standardeinstellungen begrenzen die Informationen, die angezeigt werden, auf Deine Schule, Deinen von Dir spezifizierten Ort und andere angemessene Begrenzungen der Gemeinschaft, die wir Dir mitteilen.

Facebook Privacy Policy 2007:

Profilinformationen, die Du auf Facebook eingibst, stehen allen Nutzern zur Verfügung, die zu mindestens einem Netzwerk gehören, dem Du Zugriff auf die Informationen im Rahmen der „Privacy Settings" erlaubst (zum Beispiel: Schule, geografisches Umfeld, Freunde von Freunden). Dein Name, der Name Deiner Schule und Dein Profilbild sind im Rahmen der Suchfunktion im gesamten Facebook-Netzwerk auffindbar, es sei denn, Du änderst Deine „Privacy Settings".

Facebook Privacy Policy November 2009:

Facebook ist dafür ausgelegt, es Dir einfach zu machen, Informationen mit jedem zu teilen, mit dem Du teilen möchtest. Du entscheidest, wie viele Informationen Du teilen möchtest, und Du kontrollierst die Weitergabe durch die „Privacy Settings". Du solltest Dir die Standardeinstellungen ansehen und diese – falls nötig – ändern, um Deine Präferenzen abzubilden. Du solltest die Einstellungen auch beachten, wann immer Du Informationen teilst [...].

Information mit der Einstellung „alle" ist öffentlich verfügbar und kann von jedem Internetnutzer eingesehen werden (dies schließt Personen ein, die nicht auf Facebook eingeloggt sind), kann durch Suchmaschinen von Dritten indiziert werden und kann mit Deiner Person außerhalb von Facebook verknüpft werden (etwa beim Besuch von anderen Seiten im Internet) und darf durch uns und andere ohne Einschränkungen hinsichtlich der Privatsphäre importiert und exportiert werden. Der Standardwert für bestimmte Informationstypen, die Du auf Facebook bereitstellst, ist auf „jedermann" eingestellt. Du kannst die Standardeinstellungen ansehen und in Deinen „Privacy Settings" ändern.

Facebook Privacy Policy Dezember 2009:

Bestimmte Kategorien von Informationen, wie zum Beispiel Dein Name, Dein Profilfoto, Deine Freundesliste und Seiten, von denen Du ein Fan bist, Geschlecht, Herkunftsregion und Netzwerke, zu denen Du gehörst, werden als öffentliche Informationen für jedermann – dies schließt mit Facebook ergänzte Applikationen ein – betrachtet und haben daher keine „Privacy Settings".

Du kannst dennoch die Möglichkeiten von anderen, diese Informationen durch Suche aufzufinden, durch Nutzung Deiner „Privacy Settings" begrenzen.

Facebook Privacy Policy, Stand April 2010:

Wenn Du Dich mit einer Applikation oder Website verbindest, erhält diese Zugriff auf „Allgemeine Informationen" über Dich. Der Begriff „Allgemeine Informationen" beinhaltet Deinen Namen und die Namen Deiner Freunde, Profilbilder, Geschlecht, Nutzer-IDs, Verbindungen und jede Art von Inhalt, der über die Einstellung „jedermann" geteilt wurde. [...] Die Standardeinstellung für bestimmte Informationstypen, die Du auf Facebook postest, ist „jedermann".

Im Mai 2010 hat die New York Times (www.nytimes.com/2010/05/13/technology/personaltech/13basics.html) nachgezählt und dabei ermittelt, dass Facebook zum Zeitpunkt der Erhebung rund 50 einzelne „Privacy Settings" vorsieht – mit circa 170 Einstellungsmöglichkeiten.

Dieselbe renommierte amerikanische Zeitung hat in einem weiteren Beitrag (www.nytimes.com/interactive/2010/05/12/business/facebook-privacy.html) zudem die Anzahl der Wörter ermittelt, die Facebooks „Privacy Statements" zum jeweiligen Zeitpunkt umfasst haben, und kam dabei auf folgende Werte:

- 2005: 1.004 Wörter,
- 2006: 2.313 Wörter,
- 2007: 3.067 Wörter,
- November 2009: 5.394 Wörter,
- Dezember 2009: 5.443 Wörter,
- Frühjahr 2010: 5.830 Wörter.

Zum Vergleich – die entsprechenden Statements bei anderen Social-Media-Websites umfassen jeweils folgende Wortanzahl:

- 384 bei Flickr,
- 1.203 bei Twitter,
- 1.977 bei Friendster,
- 2.290 bei Myspace,
- (5.830 bei Facebook, siehe oben).

Zusammenfassend lässt sich sagen: Die Privatsphäre eines Nutzers bei Facebook steht permanent unter Druck. Die wiederholten einseitigen Änderungen von Facebook sind kein Zeichen einer „Ausprobier-Mentalität" eines Start-ups, sondern schaffen die unabdingbare Grundlage für

das eigentliche Geschäftsmodell von Facebook (und vieler anderer Web-2.0-Unternehmen): der Verwertung von Nutzerdaten, etwa durch den Verkauf von Nutzerprofilen an werbetreibende Unternehmen.

Was Facebook über Nicht-Nutzer weiß

Ist man mit dem Umgang von Facebook und anderen Diensten mit den persönlichen Daten der Nutzer nicht einverstanden, so wäre die naheliegendste Lösung, einfach wegzubleiben oder sein Profil zu löschen. Lassen wir mal den Fall des Entfernens eines existierenden Profils weg, wegen der damit verbundenen Schwierigkeiten und der offenen Frage, ob man mit einer solchen Aktion tatsächlich aus dem Datenbestand des Anbieters verschwunden ist, und konzentrieren uns nur auf die Fragestellung, was mit den eigenen Daten passieren kann, wenn man *nicht* beitritt.

Tatsächlich weiß Facebook erstaunlich viel über Nicht-Mitglieder. So ist – bei der hohen Nutzerzahl – nicht unwahrscheinlich, dass andere Mitglieder, die Sie persönlich (offline) kennen, Informationen über Sie veröffentlichen, etwa Fotos hochladen, auf denen Sie zu sehen und genannt sind, oder – es ist ja so einfach – Facebook den Zugriff auf das Computer- oder Handyadressbuch erlauben, in dem auch Ihre Kontaktdaten gespeichert sind.

Voilà, damit sind Sie auch drin im Datenbestand von Facebook. Tauchen Sie bei verschiedenen Mitgliedern noch mehrfach auf, liefern Sie Facebook sogleich auch ungewollt Daten über Ihr persönliches Kontaktnetzwerk. Und das alles, ohne überhaupt Mitglied zu sein. Ein Entkommen ist praktisch unmöglich. Sie können lediglich Ihre Kontakte bitten, die Inhalte zu entfernen, oder – wie es manchmal empfohlen wird – selbst Mitglied zu werden, um vielleicht etwas besser steuern zu können, was über Sie veröffentlicht wird.

Was uns noch bevorsteht

Noch ist die Facebook-Gesichtserkennung in der Betaphase, aber schon bald soll die Software so weit sein, bei hochgeladenen Personenfotos automatisch Personen wiederzuerkennen. Ein einziges mit einer Person in Verbindung gebrachtes Foto reicht dann aus, um eine Person zu identifizieren und aus Millionen von Fotos diejenigen herauszusuchen, die diese Person zeigen. Das ist nicht nur aus Nutzersicht ungemein praktisch, sondern verschafft dem Anbieter ganz neue Perspektiven über soziale Zusammenhänge, selbst wenn die nicht explizit durch „Freundschaftsanfragen“ und Kommentare ersichtlich sind.

Weitere Transparenz liefert die kürzlich gestartete Facebook-Suchfunktion, die nicht nur in Facebook, sondern auch über Partnerseiten hinweg suchen kann.

Und die anderen Plattformen?

Facebook steht durch die Aufweichung der Privatsphäre zunehmend in der Kritik. Darüber hinaus wird oft vergessen, dass andere Anbieter auf ähnlicher Basis arbeiten und ebenso Daten sammeln. Aus fehlender öffentlicher Diskussion darf man daher keinesfalls den Schluss ziehen, alles wäre bei StudiVZ und Co in bester Ordnung.

Cyberstalking – es kann jeden treffen

Auch wenn man stets vorsichtig mit seinen Daten ist, kann man als Nutzer ganz unerwartet in Schwierigkeiten geraten, etwa als Opfer gezielter Online-Mobbing-Aktionen.

Psychoterror per Internet

Von Haus aus bringen einige Dienste wie „meinprof“, „Spickmich“ oder „Don’tdatehimGirl“ etc. erhebliches Missbrauchspotential mit, wie zum Teil bereits beschrieben wurde. Onlinemobbing, Cybermobbing oder auch Cyberbullying und Cyberstalking sind die Begriffe für das unerwünschte Bedrängen einer anderen Person mit Hilfe des Internets, also etwa in Foren, in Chatrooms oder in Social Networks.

Mobbing ist seit Jahren ein primär aus der Arbeitswelt, aber auch aus dem schulischen Umfeld bekannter Begriff, der auch im Internetkontext verwendet wird. Eine Abgrenzung zum Stalking ist – im Onlineumfeld – nicht leicht. Nachfolgend werden die Begriffe synonym verwendet.

Die besuchenswerte Website Computerbetrug.de widmet sich ausführlich und fundiert dem Thema. Cyberstalking ist demnach ein kriminelles Phänomen, das den Ruf eines Menschen aufs Übelste beschädigen kann. Der Begriff Stalking kommt aus dem Englischen und bedeutet übersetzt so viel wie Heranpirschen oder Belauern. Im übertragenen Sinn versteht man unter Stalking, wenn ein Mensch einen anderen massiv und dauerhaft unter psychischen Druck setzt, ihm also auflauert, ihn unerwünscht kontaktiert oder ihn verfolgt. In unserer Betrachtung eben mit Mitteln des Internets und Web 2.0.

Zu den Mitteln zählen das Verbreiten von Gerüchten, das Hochladen von Fotos und Videos, die den Betroffenen in bloßstellender Form zeigen, aber auch die bewusste Falschbewertung von Produkten und Leistung.

Die Motive für diese Form des Psychoterrors sind vielfältig: Unerwiderte Liebe zählt ebenso dazu wie Rache, Neid, Hass, verletzte Ehre oder auch eine psychische Störung des Täters. In der Mehrzahl der beobachteten Fälle sind oder waren Täter(in) und Opfer nach Angaben von Computerbetrug.de vor Beginn des Stalkings persönlich oder intim bekannt. Es gibt jedoch auch andere Fälle. So sind Prominente unter Umständen auch online das Opfer von „Fans". Auch aus dem Literaturbetrieb wird häufig berichtet, dass Autoren die vermeintliche Konkurrenz schon mal mit schlechten Kritiken zu diskreditieren versuchen.

Das Internet oder andere digitale Kommunikationsmedien werden beim Cyberstalking instrumentalisiert, um das Opfer psychisch unter Druck zu setzen oder ihm in anderer Form zu schaden. Praktisch immer operieren die Täter unter dem Deckmantel einer (scheinbaren) Anonymität und können darauf zählen, dass sie durch die große Verbreitung des Internets einen breiten Adressatenkreis erreichen – womit der psychische Druck auf ihr Opfer entsprechend größer wird.

Computerbetrug berichtet in Sachen Cyberstalking aber auch von einer gewissen Professionalisierung der Aktivitäten in diesem Sektor: „Die Täter betreiben ihr sozialschädliches Handwerk, um Menschen aus rein geschäftlichen Interessen heraus zu schaden – oder werden von Dritten dafür bezahlt, um Konkurrenten oder andere unliebsame Menschen einzuschüchtern."

Cyberstalking tritt in den unterschiedlichsten Formen auf, abhängig von der kriminellen Energie des Täters und seinen Möglichkeiten. Denkbar und praktiziert wird Cyberstalking unter anderem in Form von (nach Computerbetrug.de):

- Verbreitung von Lügen, Gerüchten oder Verleumdungen über das Opfer auf Internetseiten, in Diskussionsforen, Blogs, Newsgroups oder per Mail,
- Warenbestellungen im Namen der Opfer oder unbeteiligter Dritter, wobei die Waren dann den Opfern zugehen – oder völlig unbeteiligten Dritten –, während das eigentliche Opfer die Rechnung erhält (siehe auch: Identitätsdiebstahl),
- Veröffentlichung intimer Details (Sexualleben, finanzielle Situation, Arbeitsleben, persönliche Eigenschaften) über das Opfer,

- Veröffentlichung und Verbreitung privater Fotos („Nacktbilder“) des Opfers – etwa aus einer früheren gemeinsamen Beziehung – auf Internetseiten, in Newsgroups, Foren und in Tauschbörsen,
- Veröffentlichung und Verbreitung manipulierter Fotos des Opfers auf Internetseiten, in Newsgroups, Foren, anonymen Blogs und in Tauschbörsen,
- Kontaktierung und Belästigung des Opfers oder dessen Freunde/Bekannte/Kollegen per Mail,
- Identitätsdiebstahl, etwa durch Anmeldung des Opfers in Internetkontaktbörsen unter dessen Namen und mit dessen Bildern oder Registrierung von Fake-Accounts unter dem Namen des Opfers,
- falsche Verdächtigung und Kriminalisierung, etwa durch Begehung von Straftaten im Internet unter dem Namen des Opfers (Teilnahme an Versteigerung, Spamming, Androhung von Amokläufen oder Attentaten etc.).

Die „Königsklasse“ des Cyberstalking ist – wenn man so sagen will – mit erheblichem Aufwand verbunden. Dabei wird mit den gesammelten Daten eine falsche Identität des Opfers im Internet aufgebaut. Etwa auf einer Plattform, auf der das Opfer noch nicht vertreten ist. Aus den bekannten Fakten (Name, Adresse, Alter, Freundeskreis) und den an anderer Stelle veröffentlichten Bildern lässt sich eine neue, vermeintlich persönliche Profilseite oder Webseite des Opfers einrichten, die diese in ein neues, völlig falsches Licht rückt – etwa durch antisemitische Äußerungen in den Statusmeldungen. Der Schaden, der hier einer Person droht, insbesondere wenn diese in der Öffentlichkeit steht, ist erheblich.

Cyberstalking scheint inzwischen ein Massenphänomen zu sein. In Österreich wird etwa jeder Fünfte durch „Cyberstalking“ belästigt. Das hat eine Studie der Donau-Universität Krems und der Universität Wien zum Thema „Cyberstalking“ ergeben. Befragt wurden 747 Personen nach repräsentativen Kriterien im Alter von 18 bis 66 Jahren. Demnach wurden 2,7 Prozent der Befragten virtuell belästigt, indem unerwünschte Informationen über sie im World Wide Web beziehungsweise in Social Networks verbreitet wurden. Am weitaus häufigsten ist aber das Stalken von Privatpersonen mittels SMS und Mails und zu einem geringeren Teil mittels Nachrichten in Social Networks. Nach der Studie sind die Täter häufig Ex-Partner, die Opfer – und das ist eines der überraschenden Ergebnisse der Studie verglichen mit der vorherrschenden Meinung anderer Untersuchungen – in etwa zu gleichen Teilen Frauen und Männer.