Der „gläserne Bürger“ im Web 2.0

Herausforderungen des „virtuellen Striptease“

DOI 10.1007/s11576-010-0230-6

Die Autoren

Prof. Dr. Hans Ulrich Buhl (✉)
FIM Kernkompetenzzentrum Finanz- & Informationsmanagement
Universität Augsburg
Universitätsstraße 12
86159 Augsburg
Deutschland
hans-ulrich.buhl@wiwi.uni-augsburg.de

Prof. Dr. Günter Müller
Institut für Informatik und Gesellschaft
Albert-Ludwigs-Universität Freiburg
Friedrichstraße 50
79098 Freiburg
Deutschland
mueller@iig.uni-freiburg.de

Online publiziert: 2010-06-24

This article is also available in English via http://www.springerlink.com and http://www.bise-journal.org: Buhl H.U., Müller G. (2010) The “Transparent Citizen” in Web 2.0. Challenges of the “Virtual Striptease”. Bus Inf Syst Eng. doi: 10.1007/s12599-010-0113-9.

Die Welle der Entrüstung über eine drohende „Sicherheits-Peepshow“ war groß, als zu Beginn dieses Jahres wieder die Forderung nach einem Aufrüsten von Flughäfen mit Nacktscannern aufkam. Eine solche angeordnete Entblößung war in vielen Augen ein nicht hinnehmbarer Verstoß gegen die Menschenwürde. Lenkt man den Blick weg von der realen hin zur virtuellen Welt, so meldete der US-Marktforscher Hitwise im März 2010, als dieses Editorial geschrieben wurde, dass – gemessen an der Anzahl der Besuche (Visits) – das Online Social Network Facebook den Suchmaschinenriesen Google als meistbesuchte US-Website abgelöst hat. Ist es nicht bemerkenswert, dass ein Großteil unserer Gesellschaft zwar Nacktscanner ablehnt, jedoch im heutigen „Mitmach-Web“ der täglichen Verlockung des gemeinsamen „virtuellen Striptease“ nicht widerstehen kann? Dabei gibt man (mehr oder weniger) freiwillig im Laufe der Zeit mehr von sich preis, als ein Nacktscanner je „enthüllen“ könnte. Besonders verlockend (und gefährlich) sind dabei die Einfachheit und Attraktivität der Geschäftsmodelle aktueller Web-2.0-Angebote wie Online Social Networks oder Weblogs: Gegen die Herausgabe persönlicher Daten „erkauft“ man sich den vermeintlich kostenlosen Zugang zu attraktiven Internetdiensten. Das Perfide daran ist, dass sich die meisten Nutzer dieses „Bezahlvorgangs“ und der potenziellen negativen Folgen nicht einmal bewusst sind.

Einige Beispiele mögen dies verdeutlichen: Das Web-2.0-Angebot Blippy (http://www.blippy.com) ist eines von vielen, die vom freiwilligen „virtuellen Striptease“ leben. So werden dort durch die Angabe der Kreditkartennummer und/oder der Zugangsdaten zu Onlineshops, wie z. B. Amazon oder Ebay, sämtliche Einkaufstransaktionen (inkl. entsprechender Details) dem jeweiligen Nutzerprofil zugeordnet. Analog zum Twitter-Prinzip kann somit verfolgt werden, wofür Freunde und Bekannte ihr Geld ausgeben, und jede Transaktion kann – wie es sich für ein „Mitmach-Angebot“ gehört – kommentiert werden. Noch tiefere Einblicke in die Aktivitäten und das soziale Umfeld eines Nutzers bieten die aktuell an Popularität gewinnenden Web-2.0-Angebote, die mittels Geodaten reale und virtuelle Welt verbinden. So nutzt bspw. Foursquare (http://www.foursquare.com) GPS-Daten, um der rasant wachsenden Anzahl an Smartphone-Nutzern ein Hybridangebot aus einem „Freunde-Radar“, einem lokalen Empfehlungsdienst, einem virtuellen Spiel und einer Plattform für ortsbasierte Werbung anzubieten. Welche Gefahren von einer derartig „spielerischen“ Verknüpfung von virtueller und realer Welt jedoch ausgehen können, zeigte sich am Beispiel von Googles jüngstem Web-2.0-Angebot „Google Buzz“ (http://www.google.com/buzz). Mit Buzz bietet Google seinen über 140 Millionen Googlemail-Nutzern nicht nur Social-Networking in Echtzeit, sondern integriert darüber hinaus die Funktionalität u. a. von Mailprogramm, Twitter-Dienst, Fotoalbum, Videoplattform und Newsreader. Der Clou beim Launch lag dabei im automatischen Erstellen von Freundeslisten auf der Grundlage bereits vorhandener Googlemail-Kontakte. Diese „Freunde“ erhielten automatisch, d. h. ohne vorherige Freigabe durch das betroffene Buzz-Mitglied, Einblicke in dessen Privatsphäre (u. a. private E-Mail-Kontakte). Darüber hinaus wurden ihnen die normalerweise unter einem Pseudonym veröffentlichten Blogeinträge, Twitter-Nachtrichten („tweets“) und Statusmeldungen des Nutzers direkt in einem „Ticker“ angezeigt. Was sich zunächst als sehr hilfreich und praktisch darstellte – so entfiel das lästige Kontaktieren und Kontaktbestätigen von Freunden – konnte jedoch weitreichende negative Folgen haben. Dies zeigt der Fall einer jungen US-Amerikanerin. Nachdem es ihr nach der Trennung von ihrem gewalttätigen Ehemann gelungen war, alle ihre Spuren im realen Leben zu verwischen, und ein Pseudonym im Internet Anonymität suggerierte, klassifizierte der Identifizierungsalgorithmus in Buzz auf Basis des historisch bedingten regelmäßigen Kontaktes den Ex-Ehemann als „Freund“ und zeigte ihm neben aktuellen Blogeinträgen auch den neuen Aufenthaltsort und Arbeitgeber der US-Amerikanerin an. Obwohl die Buzz-Funktion nach diesem Eklat sofort überarbeitet

wurde, ist dieses prominente Beispiel nicht als Einzelfall zu verharmlosen. Es ist nur eines unter vielen weiteren, bei denen sich die leichtfertige Preisgabe persönlicher Daten im Netz zum Stolperstein nicht nur im Privaten, sondern bspw. auch für die berufliche Karriere herauskristallisierte. Zusätzlich eröffnen neue technologische Entwicklungen, wie der sich noch aktuell in der Testphase befindende automatisierte Abgleich von digitalen Bildern, und darauf aufbauende Anwendungen immer mehr ungeahnte und potenziell unangenehme Recherchemöglichkeiten. So scheint bspw. eine Identifizierung von fremden Menschen per Handy greifbar nahe. Verknüpft und angereichert mit zahlreichen Informationen weiterer Web-2.0-Anwendungen könnten somit Fremde in Sekundenbruchteilen mehr über uns erfahren als ein Nacktscanner je enthüllen kann.

Spätestens an dieser Stelle muss man sich die Frage stellen, ob die Langzeitfolgen der Freigiebigkeit der persönlichen Daten einerseits und der rasante technologische Fortschritt im Web 2.0 andererseits für uns und unser alltägliches Leben überhaupt absehbar sind. So diskutiert man bspw. in der Versicherungswirtschaft darüber, Nutzern entsprechender Web-2.0-Angebote, die (un-)freiwillig ihren aktuellen Aufenthaltsort veröffentlichen, mit einem Prämienaufschlag bei Hausratversicherungen zu versehen oder künftig Versicherungsfälle abzulehnen, weil der Versicherte seiner Sorgfaltspflicht nicht nachgekommen ist.

Die o. g. Beispiele machen zumindest das Folgende klar: Obwohl die nahezu exponentiell steigende Nutzerzahl insbesondere ortsbasierter Web-2.0-Angebote für den (zumindest temporären) individuellen Nutzen sprechen, vernachlässigen die Nutzer, dass sie wie Hänsel und Gretel im Märchen durch „digitale Brotkrumen" potenziell für immer eine Spur hinterlassen, die fast in Echtzeit mit anderen historischen Spuren verknüpft werden kann. Im Märchen wurden die Brotkrumen von Vögeln gefressen – im Web 2.0 passiert das bestimmt nicht. Fälle wie der der jungen US-Amerikanerin zeigen exemplarisch, welche Folgen die Verletzung der Privatsphäre und die Verknüpfung von Daten aus unterschiedlichen Quellen haben können.

Die interessanten Fragen aus heutiger Sicht sind daher: Welche allgemeinen Entwicklungen sind über die o. g. Beispiele hinaus erkennbar? Welche Gefahren und Herausforderungen resultieren daraus für Individuen, Unternehmen und die Gesellschaft?

Diese Fragen sind umso wichtiger, als die aktuellen Entwicklungen im Web 2.0 nur ein kleiner – wenn auch bedeutender – Schritt hin zu einer digitalen Identifizierung sind. So werden durch die zunehmende Informatisierung der realen Welt z. B. durch RFID und „Ubiquitous Computing", durch neue Software-Applikationen wie „Google Goggles" (http://www.google.com/mobile/goggles) oder das kontrovers diskutierte „Google-Streetview" (http://maps.google.de/help/maps/streetview) bereits heute riesige Datenmengen gespeichert. Zwar wird dieser Informatisierung und Vernetzung eine entscheidende Rolle bei der Lösung grundlegender zukünftiger Menschheitsprobleme (Ressourcenknappheit, Klimaerwärmung, demographischer Wandel, unkontrollierte Migration, Verkehrskollaps, Terrorismus etc.) zugesprochen. Jedoch gelangen dadurch weitere sensitive Daten, deren Verwendung nicht mehr von uns kontrolliert oder beeinflusst werden kann, in die Hände weniger Internetgiganten. So werden zukünftig neben unseren Telefonaten, Kreditkarten, E-Mail- und Internet-Konten selbst Kleidungsstücke und Fahrkarten Informationen über uns erfassen.

Welche Auswirkungen in diesem Zusammenhang das vieldiskutierte „Cloud Computing" hat, soll hier nur kurz andiskutiert werden: „Cloud-Computing" und die Dienstorientierung scheinen sich als neue Konzepte für ein globales und standardisiertes Angebot herauszukristallisieren. „Rechnen auf Nachfrage" reduziert dabei zumindest in der Theorie zusammen mit den Möglichkeiten der neue Dienste und der Dienstkomposition den Grundaufwand für die IT in einem bisher unvorstellbaren Maße. So bietet bspw. Google bereits heute E-Mail-Konten und enormen Speicherplatz für Daten, Videos und Graphiken für 30 € im Monat an, ein Angebot, das kein heutiges Rechenzentrum leisten kann. Unternehmen sind hingegen (noch?) zurückhaltend, da komplexe Anwendungen wie Geschäftsprozesssysteme nicht so weit transferierbar sind, dass man sie einer „Cloud" anvertrauen möchte. Die entsprechende Bedeutung hinsichtlich der damit verbundenen Speicherung persönlicher Daten auf virtuellen, vom privaten Dienstleistern betriebenen Riesencomputern, für den Schutz unserer Privatsphäre führt womöglich den „virtuellen Striptease" in derzeit nicht vorstellbare Sphären.

Eines wird dabei deutlich: Durch eine Bündelung der zahlreichen digitalen Spuren, die wir somit im Laufe der Zeit on- und offline hinterlassen, wird ein immer feineres

und detaillierteres Mosaik unserer realen Existenz entstehen, die George Orwells Überwachungsfiktion „1984“ Realität werden lässt – jedoch anders, als er sich das vorgestellt hat.

Das Problem ist nämlich nicht der „gläserne Bürger“, der machtlos dem „Überwachungsstaat“ ausgeliefert ist, sondern dass uns kein Staat der Welt mehr vor der drohenden Anarchie im Netz schützen kann. Denn längst scheinen die größten Datensammler wie Google, Facebook und Microsoft u. v. m. alles zu überwachen – und doch gibt es nicht wirklich einen identifizierbaren Wächter. War es hierzulande zu Volkszählungszeiten noch der Staat, gegen den man sich erfolgreich wehren konnte, sind wir heute vielmehr davon abhängig, wie die Internetgiganten ihre Verantwortung begreifen. Obwohl diese beteuern, ausschließlich an der Gesamtheit der Nutzerspuren insbesondere für die Erkennung von Trends, Neigungen und Mustern und somit nicht an individuellen Daten interessiert zu sein, kann sich dies zukünftig – insbesondere wenn sich dadurch neue Ertragsquellen erschließen lassen – rasch ändern. Natürlich könnte man an dieser Stelle nun die Schlussfolgerung ziehen, dass die einfachste Lösung für den Schutz der Persönlichkeitsrechte in den Händen jedes Einzelnen liegt: Immerhin scheint es ja unsere Entscheidung zu sein, ob wir entsprechende Web-2.0-Angebote nutzen bzw. persönliche Daten im Netz veröffentlichen. Dies greift jedoch zu kurz. Einerseits gelangen persönliche Daten (insbesondere auch Bilder) indirekt durch den „Exhibitionismus“ Dritter in das Netz. Dabei stellt sich bereits das Aufspüren in den Tiefen des Netzes als zeitaufwendiges und fast aussichtsloses Katz- und Mausspiel dar, ganz zu schweigen von der anschließenden Beseitigung gefundener Spuren. In diesem Zusammenhang berichtete die deutsche Stiftung Warentest nach einer Untersuchung der großen Online Social Networks, dass über Alibi-Profile eingestellte Schmähungen von den Betreibern trotz eindringlicher Bitten der Geschädigten nicht zufriedenstellend gelöscht wurden. Stattdessen bekamen die „Bittsteller“ standardisierte E-Mails, welche mit der Anfrage nicht das Geringste zu tun hatten. Ähnlich reagierten die Betreiber auf die Bitte zur Herausgabe der Daten, die über das eigene Verhalten im OSN gespeichert sind – und dies obwohl die Betreiber hierzu in Deutschland rechtlich verpflichtet sind. Wer sich hingegen andererseits den aktuellen Entwicklungen gegenüber verschließt, läuft Gefahr, die Potenziale nicht auszuschöpfen sowie sich in gewisser Weise von einem an Bedeutung gewinnenden Teil unserer Gesellschaft zu verabschieden.

Bzgl. der Auswirkungen der zunehmenden Datenfreigiebigkeit und Vernetzung für Unternehmen ergeben sich neben den angepriesenen Potenzialen (u. a. Erschließung neuer Wissenspools durch in soziale Netzwerke eingebundene Mitarbeiter, Abschöpfen von Innovationspotenzialen durch die Integration von Kundenwissen in die Wertschöpfungskette) auch Herausforderungen, wie dies zahlreiche Vorfälle von Datendiebstahl und -missbrauch sowie Internetkriminalität verdeutlichen. Dieser Zwiespalt wird auch unter dem Begriff „De-Perimetrisierung“ subsumiert. So werden die ursprünglichen Verteidigungslinien des unternehmerischen IT-Netzwerkes durch den Einsatz mobiler Endgeräte sowie einer Vielzahl von Speichermedien „durchbrochen“ und ein Spagat zwischen Sicherheit und Mobilität muss vollzogen werden. Neben dieser Herausforderung sehen sich jedoch Unternehmen in jüngster Zeit zusätzlich mit einer durch die Vernetzung verschärften Gefahr potenzieller Diffamierungen konfrontiert. Ist der Informationsfluss in unternehmenseigenen bzw. unternehmensnahen Web-2.0-Anwendungen direkt steuerbar, kann insbesondere der aus einer Verbreitung von (absichtlich) negativ gestreuten Informationen resultierende Imageverlust in „nichtbeinflussbaren“ Anwendungen deshalb i. d. R. nicht abgewendet werden, da jegliche Kommentierung die Negativbotschaft aufwertet und möglicherweise nur noch bekannter macht. Die Möglichkeit der Erstellung anonymisierter Beiträge senkt hierbei nicht nur die Hemmschwelle, sondern erschwert auch die Rückverfolgung des auch im privaten Umfeld sowie an Hochschulen zunehmenden „Cybermobbings“.

Das Urteil des deutschen Bundesverfassungsgerichts vom März dieses Jahres, in dem die bis dahin geltende Regelung über die Speicherung von Vorratsdaten für verfassungswidrig erklärt und der Einsatz nur unter sehr strengen Auflagen ermöglicht wurde, ist vor diesem Hintergrund zweischneidig zu sehen: Einerseits reduziert das Urteil die vielleicht gar nicht so große Gefahr des Orwell'schen Überwachungsstaates für Bürger und Unternehmen. Andererseits erhöht sie zugleich die vielleicht viel größere Gefahr der kriminellen Nutzung der Anonymität: Das Verbot der Vorratsdatenspeicherung der Verbindungsdaten aus Telefon-, Mail- und Internetnutzung macht einen Schutz durch den Staat vermöge einer Rückverfolgung Internet nahezu unmöglich.

Es besteht daher eine immense gesellschaftliche Herausforderung, einerseits äußere und innere Bedrohungen abzuwehren, aber andererseits die Weiterentwicklung einer offenen Gesellschaftsstruktur nicht zu gefährden. Dabei ist auch die Rolle der IT zweischneidig: Einerseits sind neue Dienste eine unverzichtbare Koordinationstechnologie in nahezu allen denkbaren ökonomischen, politischen und sozialen Zusammenhängen (Energie- und Wasserversorgung, Produktion, Finanzwirtschaft, Gesundheitswesen, Verkehr, Ausbildung, E-Voting etc.). Aber diese Dienste bedrohen – wie dargestellt – auch die gesellschaftliche Sicherheit. Andererseits ist IT aber auch ein wichtiger „Enabler" der gesellschaftlichen Sicherheit im Sinne einer Erkennung und Abwehr von inneren und äußeren Bedrohungen. Es ist daher essenziell, dass sich jeder – sei es nun auf der Individual-, Unternehmens- oder Staatsebene – der absehbaren Auswirkungen auf seinen Verantwortungsbereich bewusst wird: Es gilt, Strategien zu einer Reduktion der diskutierten Risiken zu entwickeln ohne durch blinde Risikominimierung die innewohnenden Chancen mit zu zerstören.

Welche Maßnahmen sind also zu ergreifen, um die skizzierten Herausforderungen zu bewältigen?

- Es besteht weitgehender gesellschaftlicher Konsens darüber, dass die grundlegenden Persönlichkeits- und Freiheitsrechte von Individuen nicht dem exponentiell sich erhöhenden Datenaufkommen einer allgegenwärtigen Informationsverarbeitung zum Opfer fallen dürfen. Dies ist und bleibt ein Grundprinzip, auch wenn einerseits die teils sehr umfangreiche Herausgabe persönlicher Daten bislang freiwillig erfolgt und andererseits über das Datenschutzgesetz teilweise zu Recht gespottet wird, dass es die Technologie von vor 30 Jahren reglementiere. Hierbei ist ein gesamtgesellschaftliches Umdenken erforderlich, bei dem nicht nur jeder einzelne Nutzer an sich, sondern auch der Staat gefordert ist, den neuen Entwicklungen im Web 2.0 Rechnung zu tragen. Dabei gilt es, neben einem Diskurs über die aktuellen Herausforderungen und insbesondere darüber, was Datenschutz und Persönlichkeitsrecht im Zeitalter des Web 2.0 eigentlich bedeuten, sich nicht darauf zu verlassen, dass sich die Anbieter der Web-2.0-Angebote ihrer Verantwortung bewusst sind und entsprechend handeln. Vielmehr müssen – international koordiniert – die Anbieter aufgefordert werden, direkte Maßnahmen für den Schutz der Privatsphäre ihrer Nutzer zu ergreifen. Voreinstellungen für die Datennutzung bei der Registrierung, die bspw. neu angelegte Profile zunächst nur für den Nutzer sichtbar machen, ist dabei ein exemplarischer Vorschlag. Die Änderung der automatischen Übertragung sämtlicher Urheberrechte zu einer Datenverwendung nur nach ausdrücklicher Einwilligung durch den Nutzer ist ein anderes Thema, bei dem – solange nichts anderes vereinbart ist – das Prinzip gelten muss, dass der Nutzer Eigentümer seiner Daten bleibt.
- Auch wenn die rasante Geschwindigkeit der technologischen Entwicklung im Web 2.0 sowie die enorme Komplexität des Themas dazu führen, dass Fehlentwicklungen meist erst sehr spät, oft zu spät, erkannt werden, müssen wir zusätzlich alles dafür tun, dass bei den Nutzern dieser Web-2.0-Angebote – insbesondere den Jugendlichen – das Bewusstsein für eine entsprechende reflektierte Weitergabe persönlicher Daten geschaffen wird. Denn die Offenherzigkeit der Nutzer bzgl. ihrer persönlichen Daten kann dadurch, dass das Internet nichts vergisst und es keine Vögel gibt, die unsere „digitalen Brotkrumen" auffressen, auch noch Jahre später unangenehme Folgen nach sich ziehen. Dazu müssen wir sicherstellen, dass bereits bei der Ausbildung in Schulen und Hochschulen eine grundlegende Medienkompetenz für den sinn- und verantwortungsvollen Umgang mit dem WWW im Allgemeinen und den Web-2.0-Angeboten im Speziellen vermittelt wird. Auch die hinter den Angeboten stehenden Unternehmen sind aufgefordert, einen wesentlichen Beitrag zu leisten, indem sie zumindest über die generellen Risiken der neuartigen Anwendungen ausreichend und bereits vor der Registrierung aufklären.

Neben diesen Aspekten steht insbesondere die Wirtschaftsinformatik als Interdisziplin in der Pflicht, hinsichtlich des viel diskutierten Problemkomplexes „Sicherheit" im Rahmen der „De-Perimetrisierung" aktuelle und zukünftige Fragestellungen zu beantworten. Dies umfasst dabei insbesondere aus informationstechnischer Sicht eine wirksame Prävention und Kontrolle sowie die Reduktion von Schwachstellen im Hinblick auf die Einhaltung der Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit von IT-Systemen. Darüber hinaus zeichnen sich bereits heute weitere herausfordernde Veränderungen ab. So rücken die sogenannten „five E" (Economy, Employment, Energy, Elderly Society, Education), die durch die Verbilligung der IT wirtschaftlicher und für

mehr Nachfrager angeboten werden können, zunehmend als vordringliche Lebensbereiche für den Einsatz neuer IT-Dienste in den Mittelpunkt. In Deutschland werden diese „five E“ zukünftig einerseits um das Themengebiet Gesundheit und andererseits – quer zu der funktionalen Sichtweise – um die zunehmende digitale Identifikation des Individuums sowie die Kontrolle der Dienste erweitert, die ein Individuum in einer zukünftigen Gesellschaft in Anspruch nimmt. Job-Karte, Patientenakte und digitaler Personalausweis stellen zusammen mit dem geplanten System ELENA – in dem bereits seit Jahresbeginn der deutsche Staat sensible Daten von mehr als 40 Millionen deutschen Arbeitnehmern sammelt – nur erste Vorboten dieser Entwicklung dar. Auf welche Weise ähnliche Entwicklungen Einfluss auf unsere Gesellschaft haben können, zeigt ein Beispiel aus Japan. Dort entwickelte sich durch die fast ausschließliche Nutzung des mobilen Telefons für nahezu alle Bereiche des Lebens (u. a. für Einkauf, Partnersuche, Kommunikation mit Arbeitgeber etc.) die Telefonnummer zum entscheidenden Identifikationsmerkmal eines Individuums. Der Spielraum, auch an kriminellen Transaktionsabwicklungen, den eine derartige Legitimation und der Nachweis, dass diese Telefonnummer über einen längeren Zeitraum von ein und derselben Person genutzt wurde, bieten, ist enorm.

Nicht zuletzt dieses Beispiel verdeutlicht, dass die mit der diskutierten informationstechnischen „Aufrüstung“ einhergehende Transformation des öffentlichen, privaten und wirtschaftlichen Umfeldes und die damit verbundenen Auswirkungen auf Verhalten und Interaktion menschlicher Individuen und der Wirtschaftssubjekte wichtige Aufgaben insbesondere der Wirtschaftsinformatik sind und bleiben werden.

Hans Ulrich Buhl
Günter Müller