International Working Group
on Data Protection
in Telecommunications

675.36.13 4. März 2008

Bericht und Empfehlung zum Datenschutz in sozialen Netzwerkdiensten

- „Rom Memorandum“ -

43. Sitzung, 3.-4. März 2008, Rom (Italien)

- Übersetzung -

Bericht

Hintergrund

„Das Hauptaugenmerk eines sozialen Netzwerkdienstes ist auf die Bildung und Bestätigung von sozialen Beziehungen im Online-Bereich von Menschen gerichtet, die Interessen und Aktivitäten teilen, oder die an der Erkundung von Interessen und Aktivitäten anderer interessiert sind, und die Nutzung von Software voraussetzt. Die meisten Dienste sind im Wesentlichen webbasiert und bestehen in einer Ansammlung unterschiedlicher Möglichkeiten für Nutzer, zu interagieren [...][1]. Insbesondere ermöglichen viele populäre Websites eine Interaktion mit anderen Nutzern (auf der Basis von selbstgenerierten persönlichen Profilen[2].

Das Aufkommen und die ständig wachsende Popularität sozialer Netzwerkdienste kündigt eine grundlegende Veränderung in Bezug auf die Art und Weise an, wie personenbezogene Daten großer Bevölkerungsgruppen in aller Welt mehr oder weniger öffentlich verfügbar werden. Diese Dienste sind in den letzten Jahren unglaublich populär geworden, insbesondere bei jungen Leuten. Sie werden aber auch zunehmend zum Beispiel im beruflichen Kontext oder für Senioren angeboten.

Die Herausforderungen, die soziale Netzwerkdienste stellen, sind auf der einen Seite nur eine weitere Variation der fundamentalen Veränderung, die die Entwicklungen des Internet in den 90er Jahren des letzten Jahrhunderts mit sich gebracht haben, in dem – unter anderem – Zeit und Raum bei der Veröffentlichung von Informationen und bei Echtzeitkommunikation aufgehoben wurden, und durch die Verwischung der Trennlinie zwischen Diensteanbietern (Autoren) einerseits und Nutzern/Konsumenten (Lesern) auf der anderen Seite.

Gleichzeitig scheinen soziale Netzwerkdienste die Grenzen dessen zu verändern, was gesellschaftlich als die Privatsphäre von Personen gesehen wird: Personenbezogene Daten über Einzelne werden öffentlich (und global) in einer nie vorher da gewesenen Weise und Menge[3] verfügbar, insbesondere riesige Mengen digitaler Bilder und Videos. Im Hinblick auf den Schutz der Privatsphäre könnte eine der grundlegendsten Herausforderungen in der Tatsache gesehen werden, dass die meisten der personenbezogenen Informationen, die in sozialen Netzwerkdiensten publiziert werden, auf Initiative der Nutzer selbst und mit ihrer Einwilligung veröffentlicht werden. Während die „traditio-

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

nelle“ Datenschutzgesetzgebung sich mit der Definition von Regeln zum Schutz der Bürger gegen unfaire oder unverhältnismäßige Verarbeitung personenbezogener Daten durch die öffentliche Verwaltung (einschließlich Strafverfolgungsbehörden und Geheimdienste), und von Unternehmen beschäftigt, gibt es nur sehr wenige Regelungen zur Veröffentlichung personenbezogener Daten auf Initiative der Betroffenen selbst, weil dies vor der Entwicklung sozialer Netzwerkdienste weder in der „Offline-Welt“ noch im Internet ein großes Problem darstellte. Außerdem ist die Verarbeitung personenbezogener Daten aus öffentlichen Quellen traditionell in der Datenschutzgesetzgebung privilegiert.

Gleichzeitig ist eine neue Generation von Nutzern entstanden: Die erste Generation, die aufgewachsen ist, während das Internet bereits existierte. Diese „digitalen Eingeborenen“[4] haben ihre eigene Art der Nutzung von Internet-Diensten entwickelt, und eigene Ansichten darüber, was sie als der privat- bzw. der öffentlichen Sphäre zugehörig empfinden. Darüber hinaus könnten sie – da die meisten von ihnen im Teenager-Alter sind – eher bereit seien, Datenschutzrisiken einzugehen, als die älteren „digitalen Einwanderer“. Generell scheint es, als seien jüngere Leute eher zur Veröffentlichung (manchmal intimer) Einzelheiten über ihr Leben im Internet bereit.

Gesetzgeber, Datenschutzbehörden wie auch Anbieter sozialer Netzwerkdienste sind mit einer Situation konfrontiert, die kein sichtbares Beispiel in der Vergangenheit hat. Während soziale Netzwerkdienste eine neue Bandbreite von Möglichkeiten für die Kommunikation und den Austausch von allen Arten von Informationen in Echtzeit bieten, kann die Nutzung solcher Dienste auch zu Gefährdungen der Privatsphäre der Nutzer (und anderer Bürger, die nicht einmal Teilnehmer an sozialen Netzwerkdiensten sind) führen.

Datenschutz- und Datensicherheitsrisiken

Die Ausbreitung sozialer Netzwerkdienste hat gerade erst begonnen. Während es bereits jetzt möglich ist, einige Risiken zu identifizieren, die mit dem Angebot und der Nutzung solcher Dienste verbunden sind, ist es sehr wahrscheinlich, dass wir gegenwärtig nur die Spitze des Eisbergs sehen, und dass sich in der Zukunft neue Nutzungen – und damit auch neue Risiken – entwickeln. Insbesondere werden neue Nutzungsformen für die in Nutzerprofilen enthaltenen personenbezogenen Daten durch die öffentliche Verwaltung (einschließlich Strafverfolgungsbehörden und Geheimdiensten[5]), wie auch durch den privaten Sektor, entwickelt werden.

Die folgende Liste von Risiken stellt nur eine Momentaufnahme dar, die möglicherweise mit der Weiterentwicklung sozialer Netzwerkdienste überarbeitet und aktualisiert werden muss.

Risiken in Verbindung mit der Nutzung sozialer Netzwerke, die bisher identifiziert worden sind, schließen die Folgenden ein:

1. *Im Internet gibt es kein Vergessen:* Die Idee des Vergessens ist im Internet nicht existent. Wenn Daten einmal publiziert sind, können sie dort sozusagen „bis in alle Ewigkeit“ gespeichert bleiben – sogar dann, wenn der Betroffene sie von der ursprünglichen Website gelöscht hat, könnten Kopien bei Dritten existieren (einschließlich Archivdienste und die „Cache-Funktion“, die von einem bekannten Suchmaschinenanbieter angeboten wird). Außerdem weigern sich einige Diensteanbieter, auf Nutzeranforderungen zur Löschung von Daten, und insbesondere von kompletten Profilen schnell (oder sogar überhaupt) zu reagieren.

2. *Der irreführende Begriff der „Gemeinschaft“:* Viele Diensteanbieter geben an, dass sie Kommunikationsstrukturen aus der „realen Welt“ in den Cyberspace übertragen. Eine häufige Aussage ist, es sei sicher, (personenbezogene) Daten auf diesen Plattformen zu veröffentlichen, weil es lediglich der Weitergabe an Informationen an Freunde (wie früher im direkten Kontakt) gleiche. Eine genauere Betrachtung von Eigenschaften einiger dieser Dienste bringt jedoch zutage, dass diese Parallele einige Schwächen hat, einschließlich dessen, dass der

Begriff des „Freundes“ im Cyberspace in vielen Fällen grundlegend von der hergebrachten Idee von Freundschaft abweicht, und dass eine Gemeinschaft sehr groß sein kann[6]. Wenn die Nutzer nicht offen darüber informiert werden, wie ihre Profilinformationen weitergegeben werden und wie sie diese Weitergabe kontrollieren können, könnten sie durch die Idee der „Gemeinschaft“, wie sie oben beschrieben ist, dazu verführt werden, gedankenlos personenbezogene Daten weiterzugeben, die sie sonst nicht weitergeben würden. Schon die Namensgebung mancher dieser Plattformen (z. B. „MySpace“) erzeugt die Illusion von Intimität im Internet.

3. *„Kostenlos“ ist vielleicht nicht „umsonst“,* wenn Nutzer vieler sozialer Netzwerke tatsächlich mit der zweckfremden Nutzung ihrer persönlichen Profildaten durch die Diensteanbieter „bezahlen“, z. B. für (zielgerichtete) Werbung.

4. *Die Speicherung von Verkehrsdaten durch Anbieter sozialer Netzwerkdienste,* die technisch in der Lage sind, jede einzelne Bewegung eines Nutzers auf ihrer Website zu speichern; die eventuelle Weitergabe personenbezogener (Verkehrs-) Daten (einschließlich der IP-Adressen von Nutzern, die in manchen Fällen zusätzlich auch Aufenthaltsinformationen darstellen können) an Dritte (z. B. für Werbung oder sogar zielgerichtete Werbung). Es ist zu beachten, dass die Daten in vielen Rechtssystemen auch an Strafverfolgungsbehörden und/oder (nationale) Geheimdienste auf deren Verlangen weitergegeben werden müssen, unter Umständen sogar einschließlich ausländischer Stellen im Einklang mit existierenden Regelungen zur internationalen Kooperation.

5. *Die wachsende Notwendigkeit, Dienste zu refinanzieren und Gewinne zu erzielen, könnte die Erhebung, Verarbeitung und Nutzung von Daten der Nutzer weiter anheizen,* wenn und soweit diese den einzigen Vermögenswert der Anbieter sozialer Netzwerkdienste darstellten. Soziale Netzwerkwebseiten sind nicht – wie vielleicht der Ausdruck „sozial“ nahe legen könnte – öffentliche Versorgungsbetriebe. Gleichzeitig wird Web 2.0 als Ganzes „erwachsen“ und es gibt einen Wechsel von startups, die manchmal von Studentengruppen mit weniger finanziellen Interessen geführt werden, zu großen internationalen Unternehmen, die sich an diesem Markt beteiligen. Dies hat zu einer teilweisen Veränderung der Spielregeln geführt, weil viele dieser Unternehmen, die an nationalen Aktienbörsen notiert sind, unter einem extremen Druck ihrer Investoren stehen, Gewinne zu erzielen und zu maximieren. Weil für viele Anbieter sozialer Netzwerke die Daten in den Nutzerprofilen und die Nutzeranzahl (in Kombination mit der Nutzungshäufigkeit) den einzigen wirklichen Verkehrswert darstellt, den diese Unternehmen haben, könnte dies zu zusätzlichen Gefahren der unverhältnismäßigen Erhebung, Verarbeitung und Nutzung personenbezogener Daten der Nutzer führen. Dabei ist auch zu beachten, dass viele Anbieter sozialer Netzwerke das Konzept der Externalisierung von Kosten des Datenschutzes hin zu den Nutzern verfolgen[7].

6. *Es könnten mehr personenbezogene Informationen weitergegeben werden als man denkt:* So könnten z. B. Fotos zu universellen biometrischen Identifikatoren innerhalb eines Netzwerks oder sogar über Netzwerke hinweg werden. Software zur Gesichtserkennung ist in den letzten Jahren dramatisch verbessert werden und wird in der Zukunft sogar noch „bessere“ Ergebnisse erzielen. Es ist zu beachten, dass, wenn einmal ein Name zu einem Bild hinzugefügt werden kann, dies auch die Privatsphäre und Sicherheit anderer, möglicherweise pseudonymer oder sogar anonymer Nutzerprofile in Gefahr bringen kann (z. B. bei Profilen in Kontaktanzeigen, die normalerweise aus einem Bild und Profilinformationen bestehen, aber nicht den wirklichen Namen des Betroffenen veröffentlichen). Die Europäische Netzwerks- und Informationssicherheitsagentur weist außerdem auf eine in der Entwicklung befindliche Technologie namens „content based image retrieval“ (CBIR) hin, die weitere Möglichkeiten zur Lokalisierung von Nutzern durch Vergleich identifizierender Bestandteile eines Ortes mit Aufenthaltsinformationen in einer Datenbank ermöglicht[8] (z. B. ein Bild, das in einem Raum an der Wand hängt, oder ein abgebildetes Gebäude). Darüber hinaus führen „soziale Gra-

phen“-Funktionen, die bei vielen sozialen Netzwerkdiensten beliebt sind, zur Offenlegung von Daten über die Beziehungen zwischen verschiedenen Nutzern.

7. *Missbrauch von Profildaten durch Dritte:* Dies ist möglicherweise das wichtigste Bedrohungspotenzial für personenbezogene Daten, die in Nutzerprofilen sozialer Netzwerkdienste enthalten sind. Abhängig davon, ob (Standard-)Einstellmöglichkeiten zum Datenschutz existieren und ob und wie diese von den Betroffenen genutzt werden, wie auch von der technischen Sicherheit eines sozialen Netzwerkdienstes, werden Profilinformationen, einschließlich Bildern (die den Betroffenen selbst, aber auch andere Personen abbilden können) im schlimmsten Fall der gesamten Nutzergemeinschaft zugänglich gemacht. Gleichzeitig existieren gegenwärtig nur sehr wenige Schutzvorkehrungen gegen das Kopieren von Daten jeglicher Art aus Nutzerprofilen und deren Nutzung zum Aufbau von Persönlichkeitsprofilen, und/oder deren Wiederveröffentlichung außerhalb des sozialen Netzwerkdienstes[9].

   Aber sogar die „normale“ Nutzung von Profildaten kann das informationelle Selbstbestimmungsrecht von Nutzern und beispielsweise auch ihre beruflichen Perspektiven in gravierender Weise beeinträchtigen[10]: Ein Beispiel, das öffentliche Aufmerksamkeit erlangt hat, ist die Durchsuchung von Nutzerprofilen von Bewerbern oder Angestellten durch Personalmanager, die sich als Standardprozedur zu entwickeln scheint: Presseberichten zufolge geben bereits heute ein Drittel aller Personalverantwortlichen an, für ihre Arbeit Daten aus sozialen Netzwerkdiensten zu nutzen, z. B. zur Überprüfung und/oder Vervollständigung von Bewerberdaten[11]. Strafverfolgungsbehörden und Geheimdienste (einschließlich solcher aus weniger demokratischen Staaten mit niedrigen Datenschutzstandards) stellen weitere Instanzen dar, die wahrscheinlich Nutzen aus diesen Quellen ziehen werden[12]. Darüber hinaus stellen einige Anbieter sozialer Netzwerkdienste Nutzerdaten über Programmierschnittstellen Dritten zur Verfügung, so dass diese Daten sich dann unter der Kontrolle dieser Dritten befinden[13].

8. *Die Arbeitsgruppe ist besonders besorgt über* weiter steigende Risiken des Identitätsdiebstahl, die durch die breite Verfügbarkeit personenbezogener Daten in Nutzerprofilen und durch die mögliche Übernahme von Profilen durch nicht autorisierte Dritte gefördert werden könnte[14].

9. *Nutzung einer bekanntermaßen unsicheren Infrastruktur:* Viel ist bereits über den Mangel an Sicherheit von Informationssystemen und –netzen einschließlich Internetangeboten geschrieben worden. Zwischenfälle neueren Datums betreffen auch bekannte Anbieter sozialer Netzwerke wie Facebook[15], flickr[16], MySpace[17], Orkut[18] und den deutschen Anbieter „StudiVZ“[19]. Obwohl die Diensteanbieter Maßnahmen zur Verbesserung der Sicherheit ihrer Systeme getroffen haben, gibt es hier immer noch Möglichkeiten zur weiteren Verbesserung. Gleichzeitig ist es wahrscheinlich, dass auch in Zukunft neue Sicherheitslücken auftauchen werden und es ist aufgrund der Komplexität der Softwareanwendungen auf allen Ebenen von Internetdiensten[20] unwahrscheinlich, dass 100%ige Sicherheit jemals realisiert werden kann.

10. *Ungelöste Sicherheitsprobleme von Internetdiensten* tragen zu den Risiken der Nutzung sozialer Netzwerkdienste bei und könnten in bestimmten Fällen solche Risiken verstärken oder zur Entwicklung von spezifischen Spielarten dieser Risiken für soziale Netzwerkdienste führen. Ein kürzlich veröffentlichtes Positionspapier der Europäischen Netzwerk- und Informationssicherheitsagentur (ENISA) benennt u. a. SPAM, cross site scripting, Viren und Würmer, spear-phishing und Phising (spezifisch für soziale Netzwerke), die Infiltrierung von Netzwerken, Profil-Übernahmen und Rufschädigungen durch Identitätsdiebstahl, Stalking, Mobbing und Wirtschaftsspionage (d. h. social engineering-Angriffe unter Nutzung von sozialen Netzwerkdiensten)[21]. Nach Aussage von ENISA stellen Aggregatoren für soziale Netzwerke („social network aggregators“) ein zusätzliches Sicherheitsrisiko dar[22].

11. *Die Einführung von Interoperabilitätsstandards und Anwendungsprogrammierungs-Schnittstellen* (Application Programming Interfaces – API; z. B. „open social“, das von Google im November 2007 vorgestellt wurde), um verschiedene soziale Netzwerkdienste technisch interoperabel zu machen, enthalten zusätzliche neue Risiken: Sie erlauben die automatische Auswertung aller sozialen Netzwerke, die diesen Standard implementieren. Die API liefert buchstäblich die gesamte Funktionalität zur automatischen Auswertung, die auch in der Web-Schnittstelle implementiert ist. Mögliche Anwendungen, die das Potenzial für Rückwirkung auf die Privatsphäre der Nutzer haben (und möglicherweise auch für die Privatsphäre von Nicht-Nutzern, deren Daten Teil eines Nutzerprofils sind) könnten beinhalten: Die globale Analyse von (beruflichen und privaten) Nutzerbeziehungen, die sehr wohl „Grenzen“ zwischen verschiedenen Netzwerken überschreiten können, in denen Nutzer in verschiedenen Rollen agieren (z. B. beruflich orientierte gegenüber mehr freizeitorientierten Netzwerken). Interoperabilität könnte auch das Herunterladen und die Verwendung von Profilinformationen und Fotos durch Dritte fördern, sowie die Erstellung von Aufzeichnungen über Veränderungen in Nutzerprofilen (einschließlich des Verfügbarmachens von Informationen, die ein Nutzer aus seinem Profil gelöscht hat).

Empfehlungen

Gestützt auf das oben Gesagte gibt die Arbeitsgruppe die folgenden (vorläufigen) Empfehlungen für Gesetzgeber, Anbieter und Nutzer von sozialen Netzwerkdiensten:

<u>*Gesetzgeber*</u>

1. *Einführung eines optionalen Rechts auf pseudonyme Nutzung – d. h. in einem sozialen Netzwerkdienst unter einem Pseudonym zu handeln*[23] - wo dies nicht bereits Teil des Regulierungsrahmens ist.

2. *Es muss sichergestellt werden, dass Diensteanbieter in ehrlicher und klarer Weise darlegen, welche Daten für den Basisdienst erforderlich sind, so dass die Nutzer eine informierte Wahl treffen können, ob sie den Dienst in Anspruch nehmen wollen,* und dass Nutzer jegliche zweckfremde Nutzung (wenigstens durch Widerspruch) ablehnen können, insbesondere zum Zwecke von (zielgerichteter) Werbung. Dabei ist zu beachten, dass hinsichtlich der Einwilligung von Minderjährigen besondere Probleme bestehen[24].

3. *Einführung einer Verpflichtung für Anbieter sozialer Netzwerkdienste zur Benachrichtigung bei Sicherheitsvorfällen.* Nutzer sind nur dann in der Lage, insbesondere mit den steigenden Risiken von Identitätsdiebstahl umzugehen, wenn sie über jegliche Datensicherheitsvorfälle unterrichtet werden. Eine solche Maßnahme würde gleichzeitig dazu beitragen, ein besseres Bild darüber zu erhalten, wie gut Unternehmen Nutzerdaten sichern, und ihnen einen zusätzlichen Anreiz liefern, ihre Sicherheitsmaßnahmen weiter zu optimieren.

4. *Überdenken des gegenwärtigen Regulierungsrahmens im Hinblick auf die Verantwortlichkeit* in sozialen Netzwerkdiensten veröffentlichte personenbezogene Daten (insbesondere für personenbezogene Daten Dritter) mit Blick darauf, möglicherweise den Anbietern sozialer Netzwerkdienste ein Mehr an Verantwortlichkeit für personenbezogene Daten auf sozialen Netzwerk-Webseiten zuzuweisen.

5. *Verbesserung der Integration von Datenschutzkenntnissen im Bildungssystem.* So wie die online Veröffentlichung personenbezogener Daten Teil des täglichen Lebens besonders junger Menschen wird, müssen Datenschutz und Instrumente zum informationellen Selbstschutz Teil der Schul-Lehrpläne werden.

Anbieter von sozialen Netzwerkdiensten

Anbieter sollten ein vitales Eigeninteresse an der Datensicherheit und dem Schutz personenbezogener Daten ihrer Nutzer haben. Ein Versäumnis schneller Fortschritte in diesem Bereich könnte zum Verlust des Vertrauens der Nutzer (das bereits jetzt durch kürzliche Datenschutz- und Datensicherheitsvorfälle beträchtlich erschüttert ist) und damit sehr wohl zu einem ökonomischen Rückschlag führen, der mit der Krise vergleichbar ist, die die digitale Wirtschaft in den späten 90er Jahren erschütterte.

1. *Verständliche und offene Informationen der Nutzer* ist eines der bedeutendsten Elemente jeglicher fairen Verarbeitung und Nutzung personenbezogener Daten. Während die Notwendigkeit eines solchen Mechanismus in den meisten nationalen, regionalen und internationalen Regulierungsinstrumenten zum Datenschutz anerkannt ist, muss u. U. die gegenwärtige Form, in der viele Diensteanbieter ihre Nutzer informieren, erneut überdacht werden: Gegenwärtig – und in vielen Fällen im Einklang mit dem existierenden Regulierungsrahmen – stellen Informationen über den Datenschutz einen Teil von manchmal komplizierten und länglichen Vertragsbedingungen des Diensteanbieters dar. Zusätzlich wird manchmal eine Datenschutzinformation angeboten. Manche Diensteanbieter legen nahe, dass der Prozentsatz der Nutzer sehr klein ist[25], die diese Informationen tatsächlich herunterladen. Selbst wenn diese Information dem Nutzer zum Zeitpunkt der Registrierung auf dem Bildschirm angezeigt wird und auf Wunsch des Nutzers auch später abgerufen werden kann, könnten dem Ziel der Information der Nutzer über mögliche Konsequenzen ihres Handelns während der Nutzung des Dienstes (z. B. bei der Veränderung von Datenschutz-Einstellungen einer Sammlung von Bildern) besser durch eingebaute, kontext-sensitive Funktionen gedient werden, die die angemessene Information auf der Basis der Handlungen der Nutzer liefern.

   Die Nutzer sollten insbesondere Informationen über den Regulierungsrahmen enthalten, dem ein Diensteanbieter unterliegt, über ihre Rechte (z. B. auf Auskunft, Berichtigung und Löschung) im Hinblick auf ihre eigenen personenbezogenen Daten und zu dem Geschäftsmodell, das zur Finanzierung des Dienstes angewandt wird. Die Information muss auf die spezifischen Bedürfnisse der jeweiligen Zielgruppe zugeschnitten werden (besonders bei Minderjährigen), damit diese informierte Entscheidungen treffen können.

   Die Information der Nutzer sollte sich auch auf den Umgang mit Daten Dritter beziehen: Anbieter sozialer Netzwerkdienste sollten – zusätzlich zur Information ihrer Nutzer über die Art und Weise, wie sie die Daten der Nutzer behandeln – auch über Ge- und Verbote im Hinblick darauf informieren, wie die Nutzer Daten Dritter behandeln dürfen, die in ihren Profilen enthalten sind (z. B. wann die Einwilligung eines Betroffenen vor der Veröffentlichung eingeholt werden muss oder über mögliche Konsequenzen von Regelverstößen). Besonders die riesigen Mengen von Fotos in Nutzerprofilen, auf denen Dritte abgebildet sind (in vielen Fällen sogar versehen mit Hinweisen auf den Namen und/oder das Nutzerprofil des Dritten) spielen in diesem Kontext eine Rolle, weil die gegenwärtigen Praktiken in vielen Fällen nicht mit den existierenden gesetzlichen Rahmen zur Regelung des Rechts am eigenen Bild übereinstimmen.

   Freimütige Informationen sollten auch über verbleibende Sicherheitsrisiken gegeben werden und über andere mögliche Konsequenzen der Veröffentlichung personenbezogener Daten in einem Profil, wie auch über den möglichen gesetzmäßigen Zugriff durch Dritte (einschließlich Strafverfolgungsbehörden und Geheimdiensten).

2. *Einführung der Möglichkeit, pseudonyme Profile zu erstellen und zu nutzen, und für deren Nutzung werben.*

3. *Einhaltung von Versprechungen gegenüber den Nutzern:* Eine „conditio sine qua non“ zur Förderung und zum Erhalt des Nutzervertrauens ist die klare und unmissverständliche Information darüber, wie ihre Daten durch den Diensteanbieter genutzt werden, besonders, soweit es die Übermittlung personenbezogener Daten an Dritte betrifft. Bei einigen Diensteanbietern bestehen allerdings gegenwärtig Zweideutigkeiten im Hinblick auf diese Versprechungen. Das bekannteste Beispiel ist die beliebte Aussage „Wir werden Ihre personenbezogenen Daten niemals an Dritte weitergeben“ in Verbindung mit zielgerichteter Werbung. Während diese Aussage in den Augen des Diensteanbieters formal korrekt sein mag, unterlassen es manche Anbieter, in klarer Weise die Tatsache zu kommunizieren, das z. B. für die Anzeige von Werbeeinblendungen in dem Browser-Fenster eines Nutzers die IP-Adresse dieses Nutzers an einen anderen Diensteanbieter, der den Inhalt der Werbung liefert, weitergegeben werden könnte. Dies geschieht in manchen Fällen gestützt auf Informationen aus dem Profil eines Nutzers, die der Anbieter des sozialen Netzwerkdienstes verarbeitet. Während die Profilinformation selbst möglicherweise tatsächlich nicht an den Werbeanbieter weitergegeben wird, wird sehr wohl die IP-Adresse des Nutzers übermittelt[26] (falls der Anbieter des sozialen Netzwerks nicht z. B. einen Proxy-Mechanismus nutzt, um die IP-Adresse des Nutzers gegenüber dem Werbeanbieter zu verbergen). Einige Anbieter sozialer Netzwerkdienste nehmen irrtümlich an, dass es sich bei IP-Adressen nicht um personenbezogene Daten handelt, während dies in den meisten Rechtsordnungen tatsächlich der Fall ist. Solche Mehrdeutigkeiten können Nutzer irreführen, und eine Erosion des Vertrauens befördern, wenn die Nutzer erfahren, was wirklich passiert. Dies ist weder im Interesse der Nutzer, noch im Interesse des Diensteanbieters. Vergleichbare Probleme existieren hinsichtlich der Nutzung von Cookies.

4. *Datenschutzfreundliche Standardeinstellungen* spielen beim Schutz der Privatsphäre der Nutzer eine Schlüsselrolle: Es ist bekannt, dass nur eine Minderheit von Nutzern Veränderungen an Standardeinstellungen einschließlich der Datenschutzeinstellungen vornimmt, wenn sie sich bei einem Dienst anmelden. Die Herausforderung für die Diensteanbieter liegt dabei darin, Einstellungen zu wählen, die standardmäßig einen hohen Grad an Schutz der Privatsphäre bieten, ohne den Dienst unbenutzbar zu machen. Gleichzeitig ist die Benutzerfreundlichkeit der Einstellmöglichkeiten entscheidend dafür, die Nutzer zu Änderungen zu ermutigen. In jedem Fall sollte die Nicht-Indexierbarkeit von Profilen durch Suchmaschinen als Standard eingestellt sein.

5. *Verbesserung der Nutzerkontrolle über die Nutzung von Profildaten:*

- *Innerhalb der Gemeinschaft;* z. B. indem die Sichtbarkeit ganzer Profile und von in den Profilen enthaltenen Daten begrenzt werden kann, wie auch die Begrenzung der Sichtbarkeit in Bezug auf Suchfunktionen innerhalb des Netzwerks. Die Kennzeichnung von Fotos (d. h. das Hinzufügen von Links auf existierende Nutzerprofile oder des Namens der abgebildeten Person(en) sollte an die vorherige Einwilligung der Betroffenen gebunden sein.

- *Schaffung von Möglichkeiten, die eine Kontrolle der Nutzer über die Nutzung von Profildaten durch Dritte erlauben – dies ist* unerlässlich, um insbesondere Risiken des Identitätsdiebstahls zu begegnen. Im Augenblick existieren allerdings nur begrenzte Möglichkeiten zur Kontrolle von Informationen, nachdem diese veröffentlicht sind. Die Erfahrungen der Film- und Musikindustrie mit Technologien zur digitalen Rechteverwaltung legt nahe, dass die Möglichkeiten in dieser Hinsicht auch in Zukunft begrenzt bleiben könnten. Trotzdem sollten Diensteanbieter Forschungsaktivitäten in diesem Bereich verstärken: Existierende und möglicherweise vielversprechende Ansätze sind u. a. Forschungsvorhaben zum „semantischen“ oder „policy-aware web“[27], die Verschlüsselung von Nutzerprofilen, die dezentrale Speicherung von Nutzerprofilen (z. B. bei den Nutzern selbst), die Nutzung von Wasserzeichen-Technologien für Fotos, die Nutzung von Grafiken anstatt von Text für die Anzeige von Informationen und die Einführung eines Verfallsdatums, das Nutzer für ihre eigenen Profildaten setzen können[28]. Diensteanbieter sollten

außerdem danach streben, die zweckfremde Nutzung insbesondere von Bildern zu verhindern, indem sie den Nutzern eine Funktion zur Verfügung stellen, die die Pseudonymisierung oder sogar Anonymisierung von Bildern ermöglicht[29]. Sie sollten darüber hinaus effektive Maßnahmen zur Verhinderung des Durchsuchens und des massenweisen Herunterladens von Profildaten treffen. Insbesondere sollten Nutzerdaten durch (externe) Suchmaschinen nur dann durchsucht werden können, wenn der Nutzer seine ausdrückliche, vorherige und informierte Einwilligung gegeben hat.

- *Ermöglichung der Nutzerkontrolle über die zweckfremde Nutzung von Profil- und Verkehrsdaten;* z. B. für Werbezwecke, als Minimum: ein Widerspruchsrecht für allgemeine Profildaten, eine Einwilligung für sensitive Profildaten (z. B. politische Überzeugungen, sexuelle Orientierungen) und für Verkehrsdaten. Viele existierende Rechtsrahmen enthalten bindende Regelungen für die zweckfremde Nutzung für Werbezwecke, die von Anbietern sozialer Netzwerke eingehalten werden müssen. Sie sollten in Betracht ziehen, die Nutzer selbst darüber entscheiden zu lassen, welche ihrer Profildaten sie für zielgerichtete Werbung genutzt sehen wollen. Zusätzlich sollte die Einführung einer Gebühr nach Wahl des Nutzers als weitere Möglichkeit erwogen werden, um den Dienst dadurch, anstatt durch die Nutzung von Profildaten für Werbezwecke zu finanzieren.

- *Einhaltung der Rechte von Nutzern, wie sie in nationalen, regionalen und internationalen Rechtsrahmen zum Datenschutz anerkannt sind;* einschließlich des Rechts der Betroffenen auf zeitnahe Löschung ihrer Daten (dabei kann es sich auch um ganze Nutzerprofile handeln).

- *Berücksichtigung von Problemen, die im Falle der Übernahme oder des Zusammenschlusses von Unternehmen auftreten kann, die soziale Netzwerkdienste anbieten:* Einführung von Garantien für Nutzer, dass der neue Eigentümer gegenwärtige Datenschutz- (und Datensicherheits-) standards beibehält.

6. *Angemessene Mechanismen zur Behandlung von Beschwerden* sollten eingeführt werden (z. B. das „Einfrieren“ angefochtener Informationen, oder von Bildern), wo diese nicht bereits existieren, sowohl für Nutzer sozialer Netzwerke, aber auch in Bezug auf personenbezogene Daten Dritter. Wichtig ist eine zeitnahe Rückmeldung an die Betroffenen. Maßnahmen könnten auch ein Bestrafungsmechanismus für missbräuchliches Verhalten in Bezug auf Profildaten anderer Nutzer und personenbezogene Daten Dritter beinhalten (einschließlich des Ausschlusses von Nutzern von einem Dienst, soweit es angemessen ist).

7. *Verbesserung und Erhaltung der Sicherheit von Informationssystemen.* Nutzung anerkannter Methoden („best practices“) bei der Planung, Entwicklung und dem Betrieb sozialer Netzwerk-Anwendungen, einschließlich unabhängiger Zertifizierung.

8. *Entwicklung und/oder weitere Verbesserung von Maßnahmen gegen illegale Aktivitäten wie Spamming und Identitätsdiebstahl.*

9. *Angebot verschlüsselter Verbindungen für die Pflege von Nutzerprofilen, einschließlich gesicherter Anmeldeprozeduren.*

10. *Anbieter sozialer Netzwerke, die in verschiedenen Ländern oder sogar global handeln, sollten die Datenschutzstandards der Länder respektieren, in denen sie ihre Dienste anbieten.*

<u>*Nutzer sozialer Netzwerke*</u>

1. *Seien Sie vorsichtig.* Denken Sie noch einmal darüber nach, bevor personenbezogene Daten (besonders Name, Adresse oder Telefonnummern) in einem sozialen Netzwerk-Profil veröffentlicht werden. Denken Sie auch darüber nach, ob Sie mit diesen Informationen oder Bil-

dern in einer Bewerbungssituation konfrontiert werden möchten. Pflegen Sie Ihre Profilinformation. Lernen Sie von Geschäftsführern großer Unternehmen: Diese Personen kennen den Wert ihrer personenbezogenen Daten und kontrollieren sie. Deswegen werden Sie keine großen Mengen personenbezogener Informationen über diese Personen im Netz finden.

2. *Denken Sie noch einmal darüber nach, bevor Sie Ihren echten Namen in einem Profil benutzen.* Nutzen Sie stattdessen ein Pseudonym. Bedenken Sie, dass Sie selbst dann nur begrenzte Kontrollmöglichkeiten darüber haben, wer Sie identifizieren kann, weil Dritte in der Lage sein könnten, ein Pseudonym aufzudecken, besonders auf der Basis von Bildern. Erwägen Sie die Nutzung verschiedener Pseudonyme auf verschiedenen Plattformen.

3. *Respektieren Sie die Privatsphäre anderer.* Seien Sie insbesondere vorsichtig bei der Veröffentlichung personenbezogener Daten über andere (einschließlich Bildern oder sogar Bildern mit Zusatzinformationen) ohne die Einwilligung dieser Person. Bedenken Sie, dass die rechtswidrige Veröffentlichung besonders von Bildern in vielen Rechtsordnungen eine Straftat darstellt.

4. *Informieren Sie sich:* Wer bietet diesen Dienst an? Innerhalb welchen Rechtsrahmens? Gibt es einen adequaten Rechtsrahmen zum Schutz der Privatsphäre? Gibt es eine unabhängige Aufsichtsinstanz (wie z. B. einen Datenschutzbeauftragten), an den Sie sich im Fall von Problemen wenden können? Welche Garantien gibt der Diensteanbieter im Hinblick auf den Umgang mit Ihren personenbezogenen Daten? Ist der Dienst von unabhängigen und vertrauenswürdigen Einrichtungen für einen guten Schutz der Privatsphäre, und für gute Sicherheit zertifiziert worden? Nutzen Sie das Internet, um sich über die Erfahrungen anderer mit den Datenschutz- und Datensicherheitspraktiken eines Ihnen unbekannten Diensteanbieters zu informieren. Nutzen Sie vorhandenes Informationsmaterial von Anbietern sozialer Netzwerke, aber auch unabhängige Quellen wie Datenschutzbehörden[30], und Sicherheitsunternehmen[31].

5. *Nutzen Sie datenschutzfreundliche Profileinstellungen.* Begrenzen Sie die Verfügbarkeit von Informationen soweit wie möglich, insbesondere im Hinblick auf die Indexierung durch Suchmaschinen.

6. *Nutzen Sie andere Identifizierungsdaten* (z. B. Login und Passwort) als diejenigen, die Sie auf anderen Webseiten nutzen (z. B. für E-Mail oder zum Online-Banking).

7. *Nutzen Sie Kontrollmöglichkeiten* im Hinblick darauf, wie ein Diensteanbieter Ihre personenbezogenen Profil- und Verkehrsdaten verarbeitet. Widersprechen Sie beispielsweise der Nutzung für zielgerichtete Werbung.

8. *Achten Sie auf die Aktivitäten Ihrer Kinder im Internet,* insbesondere auf Webseiten sozialer Netzwerke.

Schlussbemerkung

Die Arbeitsgruppe fordert Verbraucherschutz- und Datenschutzorganisationen auf, angemessene Maßnahmen zu treffen, um Regulierer, Diensteanbieter, die Öffentlichkeit und insbesondere junge Menschen[32] auf Risiken für die Privatsphäre in Bezug auf die Nutzung sozialer Netzwerke und verantwortliches Verhalten bezüglich der eigenen personenbezogenen Daten, wie auch der Daten anderer, hinzuweisen.

Die Arbeitsgruppe wird zukünftige Entwicklungen bei sozialen Netzwerkdiensten im Hinblick auf den Schutz der Privatsphäre beobachten und diese Empfehlungen soweit notwendig überarbeiten und aktualisieren.

Anmerkungen

[1] zitiert aus Wikipedia; http://en.wikipedia.org/wiki/Social_network_service [abgerufen am 5. Februar 2008]
[2] Dieser Bericht beschäftigt sich nicht mit Chat, Blogging und Bewertungsplattformen
[3] Ein deutscher Wissenschaftler hat kürzlich in einer Auswahl populärer sozialer Netzwerkdienste ungefähr 120 einzelne persönliche Attribute identifiziert, die in Nutzerprofilen sozialer Netzwerkdienste enthalten sind, wie z. B. Name, Privatadresse, Lieblingsfilme, -bücher und –musik usw., wie auch politische Ansichten und sogar sexuelle Vorlieben. Vgl. „Berliner Morgenpost“ vom 23. Januar 2008, S. 9: „Mehr Informationen als die Stasi“; http://www.morgenpost.de/content/2008/01/23/wissenschaft/942868.html.
[4] Dieser Begriff wird Marc Prensky zugeschrieben, einem amerikanischen Redner, Autor, Berater und Spieledesigner im Bereich Ausbildung und Bildung. Vgl. z. B. http://www.ascd.org/authors/ed_lead/el200512_prensky.html [abgerufen am 5. Februar 2008]
[5] Bereits jetzt scheinen Geheimdienste in den Vereinigten Staaten von Amerika (insbesondere das „Open Source Center“, eine Dienststelle, die dem US-amerikanischen „Director of National Intelligence“ zugeordnet ist) Daten aus sog. „öffentlichen Quellen“ zu nutzen, die anscheinend unter anderem YouTube, aber auch soziale Mediendienste wie Myspace und blogs einschließen; vgl. http://www.fas.org/blog/secrecy/2008/02/open_source_intelligence_advan.html [abgerufen am 7. Februar 2008]
[6] Während einige Diensteanbieter versucht haben, begrenzte Bereiche innerhalb ihrer Dienste zu schaffen, um den Nutzern mehr Kontrolle darüber zu geben, wie sie ihre (personenbezogenen) Daten weitergeben, machen andere solche Informationen oder Teile davon einem größeren Publikum verfügbar, das in manchen Fällen in der gesamten Gemeinschaft bestehen kann – und damit in Millionen von völlig Fremden: „Zwar bleibt es unter uns“, aber „wir“ können durchaus mehr als 50 Millionen seien.
[7] vgl. die Rede von John Lawford (Canadian Public Interest Advocacy Center) beim OECD-Canada Technology Foresight Forum “Confidence, privacy and security” am 3. Oktober 2007; http://www.stenotran.com/oecd/2007-10-03-Session4b.pdf [abgerufen am 6. Februar 2008], S. 35
[8] vgl. ENISA Position Paper No. 1: „Security Issues and Recommendations for Online Social Netzworks“, October 2007, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf
[9] Dabei ist zu beachten, dass einige soziale Netzwerkdienste es Suchmaschinen gestatten, Daten ihrer Nutzer zu durchsuchen und dass in letzter Zeit Suchmachinendienste entstanden sind, die auf das Angebot von Persönlichkeitsprofilen spezialisiert sind, die aus verschiedenen Quellen zusammengestellt werden. Andererseits scheinen Diensteanbieter gegenwärtig wenig oder sogar überhaupt keine Kontrolle über die Handlungen von „Spidern“ auf ihren Websites zu haben, die das „robots.txt“-Protokoll nicht respektieren.
[10] „26. April – Eine Frau aus Pennsylvania gibt an, dass ihre Laufbahn als Lehrer durch die Universitätsverwaltung aus dem Gleichgewicht gebracht worden ist, durch unfaire Disziplinarmaßnahmen wegen eines Fotos auf MySpace, das sie mit einem Piratenhut zeigt, wie sie aus einer Plastiktasse trinkt. In einem Bundesgerichtsverfahren gibt [...] an, dass die Millersville Universität sie beschuldigt, für Alkoholkonsum Minderjähriger zu werben, nachdem sie ihr MySpace Foto entdeckt hatten, das mit ‚betrunkener Pirat’ beschriftet war“. Zitiert aus http://www.thesmokinggun.com/archive/years/2007/0426072pirate1.html [abgerufen am 11. Februar 2008]. vgl. auch „The Guardian“ vom 11. Januar 2008: „Would-be students checked on Facebook“; http://education.guardian.co.uk/universityaccess/story/0,,2238962,00.html
[11] Vgl. z. B. „Employers Use ‘Facebook’ and ‘MySpace’ to Weed Out Applicants“; http://www.wtlv.com/tech/news/news-article.aspx?storyid=644533 [abgerufen am 12. Februar 2008]. Finnland scheint bisher das einzige Land zu sein, das solche Praktiken verbietet.
[12] Andere Beispiele, die sich in der Zukunft entwickeln könnten, könnten auch die Nutzung durch Einwanderungsbehörden bei Auslandsreisen einschließen.
[13] Vgl. z. B. „Facebook API Unilaterally Opts Users Into New Services“, von Ryan Singel, 25. Mai 2007, http://blog.wired.com/27bstroke6/2007/05/facebook_api_un.html; vgl. auch Chris Soghoian: „Exclusive: The next Facebook privacy scandal“, 23. Januar 2008, http://www.cnet.com/8301-13739_1-9854409-46.html?tag=blog.1 [abgerufen am 12. Februar 2008]
[14] Vgl. als ein aussagekräftiges Beispiel z. B. die kürzlichen „Natalie“- und „frog“-Experimente, die von der Sicherheitsfirma Sophos durchgeführt worden sind; s. „Sophos Facebook ID probe shows 41% of users happy to reveal all to potential identity thieves. Research highlights dangers of irresponsible behaviour on social networking sites”, August 2007; http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html und “Der Fall 'Natalie'. Online Communities zunehmend IT-Sicherheits-Risiko. Experten warnen vor massivem Anstieg von Datendiebstahl und -missbrauch auf Social Network Websites“, 21 Januar 2008
[15] Vgl. „Secret Crush Facebook App Installing Adware, Security Firm Charges“, ‘Wired’ vom 3. Januar 2008, http://blog.wired.com/27bstroke6/2008/01/secret-crush-fa.html [abgerufen am 12. Februar 2008]

[16] Vgl. “Phantom Photos: My photos have been replaced with those of another”; http://flickr.com/help/forum/33657/ [abgerufen am 12. Februar 2008]
[17] Vgl. z. B. im Dezember 2006 “MySpace XSS QuickTime Worm”; http://www.websense.com/securitylabs/alerts/alert.php?AlertID=708 [abgerufen am 12. Februar 2008]
[18] Vgl. PC World: “Worm Hits Google's Orkut” vom 19. Dezember 2007, http://www.pcworld.com/article/id,140653-c,worms/article.html, und SC Magazine US: “Google's Orkut hit by self-propagating trojan” vom 26. Februar 2008, http://www.scmagazineus.com/Googles-Orkut-hit-by-self-propagating-trojan/article/107312/ [beide abgerufen am 3. März 2008]
[19] vgl. „Datenleck beim StudiVZ? [Update]”; http://www.heise.de/newsticker/meldung/81373/ [abgerufen am 12. Februar 2008]
[20] Außerdem wird der jährliche steile Anstieg der Menge elektronisch gespeicherter Informationen selbst als ein Sicherheitsrisiko angesehen: Bei der letzten RSA Europe Security Conference in London im Jahr 2007 wurde der RSA-Präsident Art Coviello mit der Aussage zitiert, dass allein im Jahr 2006 weltweit 176 Exabytes an Daten generiert worden seien und dass eine solch riesige Menge von Daten aus seiner Sicht nicht verwaltbar sei und nicht effektiv gesichert werden könnte; vgl. das deutsche Computermagazin „iX“, Dezember 2007, S. 22: „Trübe Aussichten: Große Datenmengen verhindern Datensicherheit“; http://www.heise.de/kiosk/archiv/ix/2007/12/022/ [abgerufen am 12. Februar 2008]
[21] ENISA Position Paper No.1: “Security Issues and Recommendations for Online Social Networks”, Oktober 2007, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf
[22] vgl. ENISA Position Paper No.1 (s. Fußnote 21), S. 12
[23] „Pseudonyme Nutzung“ bedeutet in diesem Kontext das Recht, in einem sozialen Netzwerkdienst unter einem Pseudonym zu handeln, ohne seine „wirkliche“ Identität gegenüber anderen Nutzern des Dienstes oder der Öffentlichkeit offenbaren zu müssen, wenn der Nutzer dies wünscht. Abhängig von den konkreten Umständen, kann dies sehr wohl eine Verpflichtung zur Preisgabe der wirklichen Identität gegenüber dem Anbieter eines sozialen Netzwerks bei der Registrierung einschließen.
[24] vgl. das „Arbeitspapier zum Schutz der Privatsphäre von Kindern im Netz: Die Rolle der elterlichen Einwilligung“, angenommen bei der 31. Sitzung der Arbeitsgruppe am 26./27. März 2002 in Auckland (Neuseeland); http://www.datenschutz-berlin.de/attachments/204/child_de.pdf?1177661067
[25] Ein Vertreter von Facebook erklärte kürzlich auf einer Konferenz der OECD, dass der Prozentsatz der Nutzer, die eine Datenschutzinformation abrufen, nicht höher als ein Viertel % sein könnte; vgl. http://www.stenotran.com/oecd/2007-10-03-Session4b.pdf, S. 33 f [abgerufen am 6. Februar 2008]
[26] Abhängig von den Umständen kann der Werbeanbieter sogar in der Lage sein, einige oder die gesamte dahinterliegende Profilinformation auf der Basis der Art der zielgerichteten Werbung, die einem bestimmten Nutzer angezeigt werden soll, zu rekonstruieren.
[27] vgl. z. B. Daniel J. Weitzner, Jim Hendler, Tim Berners-Lee, Dan Connolly: “Creating a Policy-Aware Web: Discretionary, Rule-based Access for the World Wide Web:, E. Ferrari and B. Thuraisingham (Herausgeber), Web and Information Security Idea Group Inc., Hershey, PA (in Erscheinen); http://www.w3.org/2004/09/Policy-Aware-Web-acl.pdf , und Sören Preibusch, Bettina Hoser, Seda Gürses und Bettina Berendt: Ubiquitous social networks – opportunities and challenges for privacy-aware user modelling; http://vasarely.wiwi.hu-berlin.de/DM.UM07/Proceedings/05-Preibusch.pdf [beide abgerufen am 12 Februar 2008].
[28] Vgl. z. B. The Royal Academy of Engineering: Dilemmas of Privacy and Surveillance. Challenges of Technological Change. März 2007, S. 40, Punkt 7.2.1
[29] vgl. ENISA Position Paper No.1: “Security Issues and Recommendations for Online Social Networks”, Oktober 2007, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf, S. 23
[30] vgl. z. B. die Broschüre “when online gets out of line” , die gemeinsam von Facebook und dem Information and Privacy Commissioner von Ontario, Canada, veröffentlicht worden ist; http://www.ipc.on.ca/images/Resources/up-facebook_ipc.pdf, den Elternratgeber der amerikanischen Federal Trade Commission: “Social Networking Sites: A Parent’s Guide”; http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec13.shtm und “Social Networking Sites: Safety Tips for Tweens and Teens”; http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec14.shtm [alle abgerufen am 3. März 2008]
[31] vgl. z. B. die von Sophos für Facebook vorgeschlagenen Datenschutzeinstellungen; http://www.sophos.com/security/best-practice/facebook.html
[32] vgl. z. B. die Kampagne „dubestemmer“, die von der norwegischen Datenschutzbehörde gestartet worden ist; http://www.dubestemmer.no/english.php, das “DADUS”-Project der portugiesischen Datenschutzbehörde; http://dadus.cnpd.pt, und die in Fußnote 30 oben aufgeführten Initiativen