

TACD

TRANS ATLANTIC DIALOGUE TRANSATLANTIQUE
CONSUMER DIALOGUE DES CONSOMMATEURS

DOC-Nr.: INFOSOC 39-09

AUSGABEDATUM: MAI 2009

Resolution zu sozialen Netzwerken

Soziale Netzwerke stellen für Millionen von Menschen ein virtuelles Zuhause dar. Sie ermöglichen Nutzern, miteinander zu interagieren, Fotos auszutauschen und sich über gemeinsame Interessen zu unterhalten. Durch soziale Netzwerke wird das Internet nicht mehr lediglich konsumiert, sondern durch jeden Einzelnen geformt. Soziale Netzwerke bedeuten jedoch auch enorme Herausforderungen für den Schutz der personenbezogenen Daten der Nutzer. Darüber hinaus werden auf sehr subtile und versteckte Weise Marketingstrategien eingesetzt, um die Nutzer, insbesondere Kinder, zu beeinflussen.

Aufgrund der Komplexität sozialer Netzwerke sind sich die meisten Nutzer der potenziellen Risiken im Zusammenhang mit der Nutzung derartiger Plattformen nicht bewusst und wissen oft nicht, wie sie sich am besten schützen können. Gleichzeitig ist es für den Einzelnen schwer, wenn nicht sogar unmöglich, sich im Rahmen von sozialen Netzwerken vorsichtig im Internet zu bewegen. Um einem sozialen Netzwerk beizutreten und dieses zu nutzen, bedarf es in den meisten Fällen der Einwilligung zur Verwendung persönlicher Daten für Marketingzwecke. Mit diesen einseitigen Vereinbarungen haben Nutzer nur eine unzureichende Kontrolle über ihre persönlichen Daten. Auf beiden Seiten des Atlantiks ist es den Regierungen bisher nicht gelungen, angemessene Schutzvorkehrungen zu treffen. So sind etwa die Safer Social Networking Principles for the EU (deutsch: Grundsätze zur Sicherheit in sozialen Netzwerken in der EU) vom Februar 2009 eher eine Absichtserklärung als eine Vorgabe eindeutiger Standards, insbesondere im Hinblick auf den Schutz personenbezogener Daten.

Empfehlungen

Nach Beschluss des TACD sollen die Regierungen der EU-Mitglieder und der Vereinigten Staaten:

1. Gesetze zum Schutz personenbezogener Daten erlassen oder abändern, um:
 - a. zu verbieten, den Beitritt zu und die Nutzung von sozialen Netzwerken von der Zustimmung des Nutzers zur Verwendung seiner Daten zu Marketingzwecken abhängig zu machen,
 - b. zu untersagen, Daten von Nutzern ohne deren ausdrückliche und freiwillige Einwilligung zu erfassen, zu verarbeiten und zu Marketingzwecken zu verwenden, wobei die Einwilligung durch Aktivieren einer entsprechenden Option (Feld anklicken) zu erteilen ist,
 - c. von sozialen Netzwerken zu verlangen, effektive und aktuelle Technologien zu verwenden, um vertrauliche persönliche Daten gegen unbefugte Nutzung zu schützen,
 - d. von sozialen Netzwerken zu verlangen, ihre Nutzer regelmäßig über die Möglichkeiten zu informieren, die diesen zum Schutz ihrer Daten zur Verfügung stehen,
 - e. von sozialen Netzwerken zu verlangen, Verantwortung zu übernehmen für den Zugriff Dritter auf von dem sozialen Netzwerk gespeicherte Daten, für den Missbrauch dieser Daten durch Dritte bzw. für Fehlverhalten Dritter im Zusammenhang mit diesen Daten,
 - f. die für Anwendungsanbieter in sozialen Netzwerken verfügbaren Informationen, die eine persönliche Identifizierung ermöglichen, auf für den Zweck der Anwendung notwendige

- Informationen zu beschränken und von Anwendungsanbietern zu verlangen, dem Nutzer mitzuteilen, welche Daten verwendet werden sollen, genau zu erläutern, zu welchem Zweck die Daten benötigt werden sowie alle Daten sofort zu löschen, sobald die Anwendung entfernt wird,
- g. von sozialen Netzwerken zu verlangen, sicherzustellen, dass von Drittanbietern erfasste Informationen, die eine persönliche Identifizierung zulassen, vom Nutzer gelöscht werden können,
 - h. von sozialen Netzwerken zu verlangen, ihre Registrierungsprozedur für Drittanbieter von Authentifizierungsdiensten, wie beispielsweise OpenID, zu öffnen
2. eine proaktive Kooperation zwischen den entsprechenden EU- und US-Behörden einleiten, um eine bessere Harmonisierung der Regulierungspraktiken und des Schutzes personenbezogener Daten zu erreichen. Dies ist vor allem deshalb von Bedeutung, weil die meisten sozialen Netzwerke auf beiden Seiten des Atlantiks tätig sind. Unterschiedliche Regulierungspraktiken sind für den Nutzer unübersichtlich und in einer globalen Umgebung von geringerer Wirksamkeit,
 3. das Bewusstsein für die möglichen Risiken der Nutzung sozialer Netzwerke, insbesondere im Zusammenhang mit dem Schutz personenbezogener Daten, fördern und die Öffentlichkeit darüber unterrichten, wie jeder Einzelne seine persönlichen Daten schützen kann. Darüber hinaus soll gefordert werden, diese Informationen auf den Seiten der sozialen Netzwerke verfügbar zu machen (Aufklärung der Verbraucher zum Schutz personenbezogener Daten),¹
 4. die Durchsetzung bestehender Vorschriften und Regelungen verbessern. Durch die mangelnde Durchsetzung ist die derzeitige EU-Politik zum Schutz personenbezogener Daten ineffektiv und vermittelt ein falsches Gefühl von Sicherheit. In den Vereinigten Staaten wird das Children's Online Privacy Protection Act (COPPA, deutsch: Gesetz zum Schutz der personenbezogenen Daten von Kindern im Internet) in der Praxis leicht umgangen. So stuft das COPPA zum Beispiel Cookies nicht als Online-Informationen ein. In der EU stehen den Behörden zum Schutz personenbezogener Daten keine ausreichenden Mittel zur Verfügung, und die möglichen Sanktionen sind eher schwach,
 5. beginnend in der OECD die Entwicklung globaler Leitlinien für Online-Werbung, verkaufsfördernde Aktionen und Direktmarketing mit der Zielgruppe Kinder in sozialen Netzwerken anregen,
 6. Forschungsarbeiten und Umfragen zum aktuellen Onlinemarketingsystem in Auftrag geben, wobei die derzeit in sozialen Netzwerken, Videokanälen, Onlinespielen und virtuellen Welten angewendeten Strategien zu ermitteln und zu beurteilen sind,
 7. durch Regulierung ausdrücklich Marketingpraktiken untersagen, für die in Forschungsarbeiten ein negativer Einfluss auf die kognitive und emotionale Entwicklung - insbesondere von Kindern - nachgewiesen wurde. Zum Beispiel sollte keine digitale Vermarktung von Lebensmittel- und Getränkeprodukten stattfinden, die zu Adipositas bei Kindern beitragen.

Die Betreiber sozialer Netzwerke sollten:

1. den Schutz und die Sicherheit personenbezogener Daten von vornherein in ihr System integrieren. Das bedeutet, dass die Standardeinstellungen möglichst wenig persönliche Informationen preisgeben und so ein Höchstmaß an Datenschutz für die Nutzer sicherstellen sollten, und dass die Websites die aktuellsten zur Verfügung stehenden Maßnahmen anwenden sollten, um Angriffe und unerwünschte Zugriffe auf Nutzerprofile zu verhindern,
2. Verbrauchern die Möglichkeit geben, die „Gewalt“ über ihre eigenen Daten zu behalten. Wenn

¹ Die Safer Social Networking Principles for the EU enthalten bereits Schritte in die richtige Richtung, behandeln jedoch nicht in ausreichendem Maße Fragen zum Datenschutz und setzen keine adäquaten Maßstäbe.
[0]http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

zum Beispiel ein Nutzer seine Mitgliedschaft beendet, sollten die gespeicherten Daten vollständig gelöscht werden. Möchte ein Nutzer selbst Daten löschen, sollte der Betreiber des sozialen Netzwerks dies nicht unnötig erschweren. Dieser Grundsatz gilt auch für Verlinkungen von Nutzerprofilen durch Nutzer oder Anwendungen: Bei jedem mit einem Nutzerprofil zu verknüpfenden Inhalt sollte per Voreinstellung zunächst der Nutzer informiert und anschließend seine Zustimmung eingeholt werden,

3. das Auslesen persönlicher Daten durch Suchmaschinen und Dritte per Voreinstellung verhindern. Ohne die ausdrückliche Einwilligung des Nutzers sollten keine Daten für Webcrawler auffindbar sein,
4. zusammen mit Verbraucherorganisationen gemeinsame ethische Grundsätze für die Verfolgung des Nutzerverhaltens und die Online-Werbung erarbeiten. Dazu sollte ein deutlich sichtbarer, eindeutiger Hinweis darauf gehören, dass die Daten zu kommerziellen Zwecken erfasst werden,
5. brancheneigene Grundsätze entwickeln, die ausführliche Vorgaben zu standardmäßig preisgegebenen Inhalten, Leitlinien für leicht verständliche Datenschutzbestimmungen sowie Regelungen zu kostenlosen Angeboten umfassen,
6. Versionen mit Werbung und Versionen ohne Verfolgung des Nutzerverhaltens zur Verfügung stellen.

Kurze Hintergrundinformationen

Einleitung

Die Inhalte und Angebote des Internets werden nicht länger einfach nur „konsumiert“. Dank des schnellen Zugangs zum Internet werden Dienste dieser Art heute interaktiv genutzt. Es ist nicht notwendig, eine persönliche Homepage zu programmieren, um persönliche Informationen bereitzustellen und mit anderen zu kommunizieren. Mit dem „interaktiven Netz“ ist es Einzelpersonen möglich, das Internet aktiv zu nutzen und daran teilzuhaben. Das virtuelle Leben wird zu einer weiteren Komponente des realen Lebens.

Im Internet gibt es hunderte von sozialen Netzwerken. Plattformen wie nasa-klasa.pl, studiVZ.de, facebook.com und myspace.com bieten ihren Mitgliedern die Möglichkeit, Informationen untereinander auszutauschen. Diese Portale ermöglichen es den Nutzern, ihre eigenen personalisierten Profildetails zu erstellen, auf denen sie zum Beispiel ihren Werdegang, Fotos, Hobbys und Kontaktdetails anzeigen, und mit anderen Nutzern Netzwerke zu bilden. Die Portale können themenorientiert sein (Musik, Autos, Tiere, Gesundheit, Sport, Bücher, Reisen) oder zielgruppenorientiert (Studenten, Schüler oder Geschäftsleute), sind jedoch in der Regel für jedermann offen. Auf einigen Portalen ist eine Registrierung nur nach Einladung durch einen anderen Nutzer möglich, der bereits Mitglied ist. Die meisten sozialen Netzwerkportale sind gebührenfrei, einige verlangen eine geringe Gebühr (z. B. sogenannte Premium-Mitglieder auf xing.com).

Zahlen und Fakten

Nach einer Studie der Universal McCann Agency vom März 2008 sind 57,5 Prozent der Internetnutzer weltweit Mitglieder in sozialen Netzwerken. In Deutschland sind es 40 Prozent. Seit 2007, als der Anteil weltweit bei 36,2 Prozent und in Deutschland bei 19 Prozent lag, sind die Zahlen rapide gestiegen. Für die Studie wurden 17000 Nutzer aus 29 Ländern befragt.²

Marktbeobachter gehen für Ende 2009 von weltweit 230 Millionen aktiven Nutzern aus. Die geschätzten Einnahmen durch soziale Netzwerke beliefen sich im Jahr 2007 auf vermutlich

² http://www.universalmccann.com/Assets/wave_3_20080403093750.pdf

956 Millionen US-Dollar; bis 2012 wird ein Anstieg auf 2,4 Milliarden US-Dollar erwartet.³

Eine Untersuchung der PricewaterhouseCoopers AG (PwC) hat ergeben, dass im Jahr 2008 71 Prozent der in sozialen Netzwerken registrierten Nutzer in mehreren Netzwerken Mitglied waren.⁴ Siebzig Prozent dieser Nutzer gaben an, „für immer“ Mitglied in ihren wichtigsten sozialen Netzwerken im Internet bleiben zu wollen. Ihre Bereitschaft, Gebühren zu zahlen, ist relativ gering, Werbung wird Mitgliedsbeiträgen vorgezogen. Die Akzeptanz von durch Werbung finanzierten Diensten liegt unserer Ansicht nach an fehlenden Kenntnissen darüber, wie Nutzerdaten analysiert werden und welchen negativen Einfluss dies auf den Schutz personenbezogener Daten haben kann. Verbraucher sollten daher Wahlmöglichkeiten haben.

Die vorliegenden Untersuchungsergebnisse und -daten zeigen deutlich die Symbiose zwischen Nutzern und Plattformbetreibern. Für den Internetnutzer hat die Mitgliedschaft in mindestens einem sozialen Netzwerk an sozialer Bedeutung gewonnen. Gleichzeitig entwickeln sich diese Plattformen zu lukrativen Einnahmequellen für die Werbebranche. Im Gegensatz zur traditionellen Werbung bieten soziale Netzwerke im Internet eine überaus effiziente Möglichkeit zur gezielten und personalisierten Werbung. Einige Netzwerke, z. B. Facebook, verwenden sogar die Profilinformationen ihrer Nutzer, um für (und auf) ihre(r) Plattform zu werben. Diese neue Form der Werbung erfordert Maßnahmen sowohl seitens der Legislative als auch der Exekutive.

Angesichts des Wettbewerbsdrucks sind die Betreiber sozialer Netzwerke gezwungen, ihren Nutzern gewisse Anreize - zum Beispiel in Form von besonderen Funktionen - zu bieten, damit diese die Plattform auch weiterhin nutzen. In der Vergangenheit gab es jedoch Kontroversen, die zeigen, unter welchem immensen Druck - sowohl aus wirtschaftlicher Sicht als auch aus Wettbewerbsperspektive - die Plattformbetreiber stehen und wie sie darum kämpfen, die Nutzer mit allen Mitteln auf ihrer Plattform zu halten. Ein Skandal betraf zum Beispiel studIVZ, deren Datenbank mit Informationen zu 2 Millionen Nutzern auf Peer-to-Peer-Plattformen veröffentlicht wurde. Die Plattform wies nicht einmal die grundlegendsten Sicherheitsfunktionen auf. Zunehmend ändern Plattformbetreiber ihre allgemeinen Nutzungsbedingungen und Datenschutzbestimmungen zum Nachteil der Nutzer bzw. zeigen ohne Einwilligung der Nutzer basierend auf deren Online-Aktivität zielgruppenspezifische Werbung an. Im März 2009 stand Facebook unter öffentlichem Druck, nachdem die Nutzer durch die neuen Nutzungsbedingungen erheblich benachteiligt worden waren. Soziale Netzwerke sind darüber hinaus ein beliebtes Ziel für Hacker und Datendiebe. Es stellt sich die Frage, ob die Plattformbetreiber ausreichend Mittel in die Sicherheit investieren oder ob die Nutzer die Kosten für den unzureichenden Schutz ihrer persönlichen Daten tragen.

Eine Studie des Fraunhofer-Instituts SIT hat gezeigt, dass die Betreiber sozialer Netzwerke beim Registrierungsvorgang eine erhebliche Menge an persönlichen Angaben verlangen, jedoch gegen einen unerwünschten Zugriff auf diese Informationen nur wenig Schutz bieten.⁵

Herausforderungen durch soziale Netzwerke

Wenngleich soziale Netzwerke ein wichtiges Instrument zur interaktiven Kommunikation darstellen und mittlerweile Teil der kulturellen Norm sind, stellen sie ihre Nutzer vor zahlreiche Herausforderungen.

Datenschutz

Grundlage des Geschäftsmodells sozialer Netzwerke ist die nicht immer transparente Nutzung der Daten registrierter Mitglieder, deren ausdrückliche Einwilligung zur Nutzung nicht

³ <http://www.cio.de/markt/uebersichten/845681/>

http://www.focus.de/digital/Internet/studie-Soziale-netzwerke-boomen_aid_299612.html

⁴ http://www.pwc.de/portal/pub/!ut/p/kcxml/04_Sj9SPykssy0xPLMnMz0vM0Y_QjzKLd4p3djUBSZhFG8Q76kfCRIL0vfV9PfJzU_UD9AtyI8odHRUVASpBSEgl/delta/base64xml/L3dJdyEvd0ZNQUFzQUMvNEIVRS82X0JfQ0VS?siteArea=49c4e4a420942bcb&content=e51fa203db61223&topNavNode=49c4e4a420942bcb

⁵ <http://www.stern.de/computer-technik/Internet/:Datensicherheit-Netzwerken-Mein-Freund-Datenh%E4ndler/636203.html>

ausdrücklich eingeholt wurde. Diese Daten umfassen von den Nutzern selbst auf ihren Profildaten gemachte Angaben sowie Auswertungen zu den Aktivitäten der Nutzer innerhalb des Netzwerks und möglicherweise auch außerhalb auf anderen Seiten im Internet. Mit diesen Daten erstellen Plattformbetreiber Nutzerprofile für eine zielgruppenorientierte, personalisierte Werbung. Ihre Datenschutzbestimmungen sind in der Regel so vage formuliert, dass Verbraucher nicht genau verstehen, wie ihre persönlichen Informationen genutzt werden. Recht üblich ist es, die Nutzung der Plattform von der Zustimmung zur Verwendung der persönlichen Daten zu Werbezwecken - entweder für Werbung durch die Plattformbetreiber selbst oder durch Dritte - abhängig zu machen. In einigen Fällen sind persönliche Profildaten nicht nur für sogenannte Freunde oder Bekannte sichtbar, sondern für jedermann. Mitunter bieten die Plattformbetreiber die Möglichkeit, den Zugriff auf die persönlichen Informationen der Nutzer einzuschränken. Häufig muss dazu jedoch eine entsprechende Option deaktiviert werden (Häkchen wegdrehen). Bisweilen wurden Nutzerdaten auch schon zu anderen Zwecken verwendet als denen, für die die Einwilligung ursprünglich erteilt wurde. Darüber hinaus sind die Daten anfällig für Angriffe durch Identitätsdiebe und Hacker.⁶

Viele Internetnutzer sind sich darüber hinaus nicht bewusst, dass das Internet „nicht vergisst“ und dass, auch wenn man meint, alle Daten seien gelöscht, diese an anderer Stelle im Netz gespeichert werden und möglicherweise sogar abrufbar sind. Die Anbieter sozialer Netzwerke haben zwar die Möglichkeit, Nutzerdaten von ihren Servern zu entfernen, jedoch tun einige dies nur sehr zögerlich.

Datenschutz ist in sämtlichen Netzwerkportalen von entscheidender Bedeutung. Bei allen kulturellen Unterschieden: Nahezu jeder Bürger steht angesichts der Herausforderungen an die traditionellen Vorstellungen von Privatsphäre vor erheblichen Problemen. Besonders Kinder verstehen nicht immer, welche Folgen die Weitergabe ihrer persönlichen Informationen haben kann und können, da minderjährig, die Einwilligung zur Verwendung ihrer Daten zu Marketing- und sonstigen Zwecken überhaupt nicht geben.⁷

Werbung

Soziale Netzwerke sind in der Regel keine gemeinnützigen Organisationen, sondern Unternehmen. Sie profitieren von zielgerichteter, personalisierter Werbung und haben zuweilen in der Vergangenheit ohne Wissen der Nutzer Informationen zu deren Kaufverhalten verwendet, um Werbung auf andere Nutzer auszurichten. Beim Kauf eines Produkts in einem mit der Plattform verknüpften Online-Shop werden unter den Schlagwörtern „vertrauenswürdige Werbung“, „Empfehlung“ alle auf der Profildaten des Käufers als Freund festgelegten Mitglieder über den Kauf informiert, damit sie das Produkt dann ebenfalls kaufen.⁸

Anwendungsentwickler

Soziale Netzwerkdienste gewähren den Entwicklern von Anwendungen einen weitaus größeren Zugriff auf Nutzerdaten, als es für die Bereitstellung der angebotenen Anwendung notwendig wäre.⁹ Diese Praktik erzeugt ein gravierendes und unnötiges Sicherheitsrisiko und verstößt gegen das Principle of Least Authority, einem Grundsatz der sicheren Gestaltung von Systemen, der besagt, dass ein Akteur stets nur die Privilegien erhalten sollte, die zur Ausführung einer Aufgabe erforderlich sind. „Anders ausgedrückt, sollte eine Anwendung, die keine privaten

⁶ <http://www.webnews.de/kommentare/137277/0/Hacker-attackieren-MySpace-Nutzer.html>
http://www.stern.de/computer-technik/Internet/Soziale-Netzwerke-Der-Spion_/641364.html
http://www.pcwelt.de/start/sicherheit/virenticker/news/187901/ein_wurm_geht_auf_myspace_und_facebook_um/
http://www.tecchannel.de/sicherheit/news/1738627/myspace_hack_musiker_seiten_verbreiten_malware/
<http://www.abzocknews.de/2008/07/14/studivz-identitatsklau-im-online-netzwerk/>
<http://www.tagesanzeiger.ch/digital/Internet/Wuermer-Hacker-Betrueger-Facebook-in-Gefahr/story/16501875>
<http://www.heise.de/newsticker/Soziale-Netzwerke-im-Visier-der-Kriminellen--/meldung/106173>

⁷ Nach dem Bericht und der Empfehlung zum Datenschutz in sozialen Netzwerkdiensten der International Working Group on Data Protection in Telecommunications, Sitzung vom 3. bis 4. März 2008 in Rom, Italien („Rom Memorandum“)

⁸ <http://www.faz.net/s/RubE2C6E0BCC2F04DD787CDC274993E94C1/Doc-E4868361D131740FBA8E380E7C7B3A8DC-ATpl-Ecommon-Scontent.html>

⁹ <http://www.cs.virginia.edu/felt/privacy>

Informationen benötigt, diese auch nicht erhalten.“¹⁰ Ähnliche Bedenken bestehen bei der Erfassung von Daten durch Werbende, die eine persönliche Identifizierung zulassen.

Kinder und Minderjährige¹¹

Betreiber sozialer Netzwerkplattformen, die ihre Dienste hauptsächlich an Kinder und Minderjährige richten, müssen derzeit grundsätzlich keine speziellen Bestimmungen zu Datenschutz oder Werbung einhalten. Hier besteht die Gefahr, dass Kinder und Minderjährige aufgrund der fehlenden Beschränkungen ausgenutzt werden. Nach einer Studie des Allensbacher Instituts für Demoskopie (IfD) aus dem Jahr 2008 ist die Hälfte aller Jugendlichen im Alter zwischen 14 und 19 Jahren in einer Online-Community aktiv.¹²

Unzureichende Maßnahmen seitens der Regierungen der EU-Mitglieder und der Vereinigten Staaten

Im Februar 2009 veröffentlichte die EU-Kommission gemeinsam mit einer Reihe von Anbietern sozialer Netzwerkdienste die Safer Social Networking Principles for the EU¹³. In diesem Dokument sind die Grundsätze dargelegt, nach denen Anbieter sozialer Netzwerkdienste dafür sorgen sollten, das Risiko einer Schädigung von Kindern und Jugendlichen so gering wie möglich zu halten. Darüber hinaus wird eine Reihe von Good-Practice-Ansätzen empfohlen. Im März 2009 brachte die Freiwillige Selbstkontrolle Multimedia-Diensteanbieter einen neuen Verhaltenskodex für die Anbieter sozialer Netzwerkdienste heraus.¹⁴ Zwar anerkennen wir die Bemühungen der EU-Kommission für einen besseren Verbraucherschutz in sozialen Netzwerken sowie die seitens der Branche eingeleiteten Initiativen, jedoch sind Verhaltensregeln und Selbstregulierungen allein nicht ausreichend, um den Herausforderungen sozialer Netzwerke zu begegnen. Angesichts der rasanten Entwicklung neuer Technologien sind Änderungen in der Gesetzgebung notwendig, und die Durchsetzung der Gesetze und Vorschriften muss verbessert werden.

¹⁰ id

¹¹ Siehe auch die Resolution des TACD Online-Marketing mit Kindern als Zielgruppe (Resolution on Marketing to Children Online, Infosoc 38-09)

¹² <http://www.spiegel.de/netzwelt/web/0,1518,584572,00.html>

¹³ http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

¹⁴ http://www.fsm.de/de/Web_2_0