

30. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre

Straßburg, 15. - 17. Oktober 2008

EntschlieÙung zum Datenschutz in Sozialen Netzwerkdiensten

Antragsteller: Berliner Beauftragter für Datenschutz und Informationsfreiheit, Deutschland

Unterstützt durch:

Commission Nationale de l'Informatique et des Libertés (CNIL), Frankreich;
Bundesbeauftragter für Datenschutz und Informationsfreiheit, Deutschland;
Garante per la protezione dei dati personali, Italien;
College Bescherming Persoonsgegevens, Niederlande;
Privacy Commissioner, Neuseeland;
Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), Schweiz

EntschlieÙung

Soziale Netzwerkdienste¹ haben in den letzten Jahre große Beliebtheit erworben. Diese Dienste bieten ihren Teilnehmern Interaktionsmöglichkeiten auf der Basis von selbst generierten persönlichen Profilen, die in einem noch nie da gewesenen Ausmaß die Veröffentlichung persönlicher Informationen zu den betreffenden Personen (und auch anderen Personen) mit sich bringen. Die sozialen Netzwerkdienste bieten zwar ein neues Spektrum von Möglichkeiten für Kommunikation und den Echtzeit-Austausch von Informationen jeder Art, die Nutzung dieser Dienste kann jedoch auch eine Gefährdung der Privatsphäre ihrer Nutzer - und Anderer - mit sich bringen, denn personenbezogene Daten einzelner Personen werden in bisher unbekannter Weise und Menge öffentlich (und global) zugänglich, einschließlich großer Mengen digitaler Fotos und Videos.

Der Einzelne läuft Gefahr, die Kontrolle über die Nutzung der Daten durch Andere zu verlieren, wenn sie erst einmal im Netzwerk publiziert sind: Während der Community-Bezug sozialer Netzwerke die Vorstellung erweckt, die Veröffentlichung der eigenen persönlichen Daten laufe in etwa auf das Gleiche hinaus, wie früher das Mitteilen von Information unter Freunden von Angesicht zu Angesicht, können Profildaten tatsächlich für alle Teilnehmer einer Community (deren Zahl in die Millionen gehen kann) verfügbar sein.

Derzeit gibt es wenig Schutz dagegen, dass personenbezogene Daten jeder Art aus Profilen kopiert werden – durch andere Mitglieder des Netzwerks oder durch unbefugte netzwerkfremde Dritte – und zum Aufbau von Persönlichkeitsprofilen verwendet werden oder dass die Daten anderweitig wieder veröffentlicht werden. Es kann sehr schwierig - und manchmal unmöglich - sein zu erreichen, dass Daten, wenn sie einmal publiziert sind, wieder vollständig aus dem Internet entfernt werden. Selbst nach ihrer Löschung auf der ursprünglichen Website (z.B. dem sozialen Netzwerk) können Kopien bei Dritten oder bei den Anbietern der sozialen Netzwerkdienste verbleiben. Personenbezogene Daten aus Nutzerprofilen können auch außerhalb des Netzwerks bekannt werden, wenn sie von Suchmaschinen indexiert werden. Hinzu kommt, dass manche Anbieter sozialer

¹ "Ein sozialer Netzwerkdienst stellt ab auf den Aufbau [...] sozialer Online-Netzwerke für Gruppen von Menschen, die gemeinsame Interessen und Aktivitäten teilen oder daran interessiert sind, die Interessen und Aktivitäten Anderer zu erkunden [...]. Die meisten Dienste sind hauptsächlich web-basiert und bieten Nutzern eine Reihe verschiedener Interaktionsmöglichkeiten [...]". Zitat aus Wikipedia: http://en.wikipedia.org/wiki/Social_network_service.

Netzwerkdienste über Applikationsprogrammierschnittstellen Drittanbietern Nutzerdaten zur Verfügung stellen, die dann unter der Kontrolle dieser Dritten stehen.

Ein Beispiel von Wiederverwendungen, das großes öffentliches Aufsehen erregt hat, ist die Praxis von Personalverantwortlichen, Nutzerprofile von Stellenbewerbern oder Angestellten zu durchsuchen. Presseberichten zufolge gibt bereits heute ein Drittel der Personalverantwortlichen an, bei ihrer Arbeit Daten aus sozialen Netzwerkdiensten zu nutzen, z. B. um die einzelnen Angaben von Bewerbern zu überprüfen und/oder zu ergänzen.

Profilinformationen und Verkehrsdaten werden von Anbietern sozialer Netzwerkdienste auch zur Weiterleitung zielgerichteter Werbung an ihre Nutzer verwendet.

Sehr wahrscheinlich werden in Zukunft noch weitere unerwartete Verwendungen von Informationen in Nutzerprofilen auftreten.

Zu weiteren, bereits jetzt identifizierten spezifischen Risiken für Datenschutz und Datensicherheit zählen erhöhte Risiken durch Identitätsbetrug, der durch die umfangreiche Verfügbarkeit personenbezogener Daten in Nutzerprofilen begünstigt wird, und durch eine mögliche Übernahme von Profilen durch unbefugte Dritte. Die 30. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre erinnert daran, dass diese Risiken bereits in dem Dokument "Bericht und Empfehlung zum Datenschutz in sozialen Netzwerkdiensten" ("Rom-Memorandum")² der 43. Tagung der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation (3. - 4. März 2008) und in dem ENISA Positionspapier Nr. 1 „Security Issues and Recommendations for Online Social Networks“³ (Oktober 2007) analysiert wurden.

Die in der Internationalen Konferenz versammelten Datenschutzbeauftragten sind von der Notwendigkeit überzeugt, dass als Erstes eine intensive Informationskampagne unter Beteiligung aller öffentlichen und privaten Interessengruppen – von Regierungsstellen bis zu Bildungseinrichtungen wie Schulen, von Anbietern sozialer Netzwerkdienste bis zu Verbraucher- und Nutzerverbänden, einschließlich der Datenschutzbeauftragten selbst – durchgeführt werden muss, um den vielfältigen mit der Nutzung sozialer Netzwerkdienste verbundenen Gefahren vorzubeugen.

Empfehlungen

In Anbetracht der besonderen Natur der Dienste und der kurz- und langfristigen Gefahren für die Privatsphäre des Einzelnen richtet die Konferenz folgende Empfehlungen an Nutzer und Anbieter sozialer Netzwerkdienste:

Nutzer sozialer Netzwerkdienste

Organisationen, denen am Wohl der Nutzer sozialer Netzwerke gelegen ist – einschließlich Diensteanbieter, Regierungen und Datenschutzbehörden – sollten mithelfen, die Nutzer über den Schutz ihrer personenbezogenen Daten aufzuklären und die folgende Botschaften zu vermitteln.

1. Veröffentlichung von Daten

Nutzer sozialer Netzwerkdienste sollten sich sorgfältig überlegen, welche persönlichen Daten sie - wenn überhaupt - in einem sozialen Netzwerkprofil publizieren. Sie sollten bedenken, dass sie zu einem späteren Zeitpunkt mit einer Information oder mit Bildern

² http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf?1208438491

³ http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

konfrontiert werden könnten, z. B. wenn sie sich um eine Arbeitsstelle bewerben. Insbesondere sollten Minderjährige vermeiden, ihre Privatanschrift oder ihre Telefonnummer mitzuteilen.

Privatpersonen sollten sich überlegen, ob es nicht ratsam wäre, in einem Profil anstelle ihres wirklichen Namens ein Pseudonym zu verwenden. Dabei sollten sie jedoch nicht vergessen, dass auch die Benutzung von Pseudonymen nur einen begrenzten Schutz gewährt, da Dritte in der Lage sein können, ein solches Pseudonym aufzudecken.

2. Die Privatsphäre Anderer

Nutzer sollten auch die Privatsphäre Anderer achten. Sie sollten besonders vorsichtig sein bei der Veröffentlichung personenbezogener Daten Anderer (einschließlich Bildern, oder sogar mit Zusatzinformationen versehenen Bildern) ohne die Einwilligung der betreffenden Personen.

Anbieter sozialer Netzwerkdienste

Anbieter sozialer Netzwerkdienste tragen eine besondere Verantwortung dafür, die Belange von Personen, die soziale Netzwerke nutzen, zu beachten und zu wahren. Sie sollten nicht nur die Regelungen des Datenschutzrechts einhalten, sondern auch die folgenden Empfehlungen umsetzen.

1. Datenschutzvorschriften und -standards

Anbieter, die in verschiedenen Ländern oder sogar weltweit tätig sind, sollten die Datenschutzstandards der Länder einhalten, in denen sie ihre Dienste betreiben. Zu diesem Zweck sollten die Anbieter Datenschutzbehörden konsultieren, wenn und soweit dies notwendig ist.

2. Aufklärung der Nutzer

Anbieter sozialer Netzwerkdienste sollten ihre Nutzer über die Verarbeitung ihrer personenbezogenen Daten transparent und offen informieren. Es sollte auch aufrichtig und verständlich über mögliche Folgen einer Veröffentlichung persönlicher Daten in einem Profil und über verbleibende Sicherheitsrisiken sowie über gesetzliche Zugriffsrechte Dritter (einschließlich z.B. von Strafverfolgungsbehörden) aufgeklärt werden. Eine solche Aufklärung sollte auch Hinweise dazu enthalten, wie Nutzer mit personenbezogenen Daten von Dritten umgehen sollten, die in ihren Profilen enthalten sind.

3. Nutzerkontrolle

Anbieter sollten die Kontrolle der Nutzer über die Verwendung ihrer Profildaten durch andere Community-Mitglieder weiter verbessern. Sie sollten die Einschränkung der Sichtbarkeit ganzer Profile sowie von in Profilen enthaltenen Daten, und in Community-Suchfunktionen ermöglichen.

Die Anbieter sollten auch eine Kontrolle der Nutzer über die Nutzung von Profil- und Verkehrsdaten, z. B. für zielgerichtete Werbung, ermöglichen. Als ein Minimum sollten eine Opt-out-Möglichkeit für allgemeine Profildaten und eine Opt-in-Möglichkeit für sensible Profildaten (z.B. politische Überzeugungen, sexuelle Orientierung) und Verkehrsdaten geboten werden.

4. Datenschutzfreundliche Standardeinstellungen

Darüber hinaus sollten Anbieter datenschutzfreundliche Standardeinstellungen für Nutzerprofilinformationen anbieten. Standardeinstellungen spielen eine Schlüsselrolle beim Schutz der Privatsphäre der Nutzer: Es ist bekannt, dass lediglich eine Minderheit von Nutzern, die sich bei einem Dienst anmelden, irgendwelche Änderungen daran vornimmt.

Diese Einstellungen müssen bei einem sozialen Netzwerkdienst, der sich an Minderjährige wendet, besonders restriktiv sein.

5. Sicherheit

Anbieter sollten die Sicherheit ihrer Informationssysteme weiter verbessern und aufrechterhalten und die Nutzer gegen betrügerische Zugriffe auf ihre Profile schützen, indem sie für die Konzeption, die Entwicklung und den Betrieb ihrer Anwendungen anerkannte Methoden einschließlich unabhängigem Auditing und unabhängiger Zertifizierung verwenden.

6. Auskunftsrechte

Anbieter sollten Personen (gleichgültig ob Mitglieder des sozialen Netzwerkdienstes oder nicht) ein Recht auf Auskunft zu ihren personenbezogenen Daten gewähren und erforderlichenfalls diese Daten berichtigen.

7. Löschung von Nutzerprofilen

Anbieter sollten den Nutzern die Möglichkeit geben, ihre Mitgliedschaft auf einfache Weise zu beenden und ihre Profile sowie alle Inhalte oder Informationen, die sie in dem sozialen Netzwerk publiziert haben, zu löschen.

8. Pseudonyme Nutzung des Dienstes

Anbieter sollten als Option die Möglichkeit der Einrichtung und Verwendung pseudonymer Profile anbieten und zur Nutzung dieser Option ermutigen.

9. Zugriff durch Drittpersonen

Anbieter sollten wirksame Maßnahmen ergreifen, um das Durchsuchen und/oder massenweise Herunterladen (oder „bulk harvesting“) von Profildaten durch Dritte zu verhindern.

10. Indexierbarkeit der Nutzerprofile

Die Anbieter sollten sicherstellen, dass Nutzerdaten von externen Suchmaschinen nur durchsucht werden können, wenn der Nutzer dazu seine ausdrückliche, vorherige und informierte Einwilligung erteilt hat. Die Nichtindexierbarkeit von Profilen durch Suchmaschinen sollte als Standard eingestellt sein.