Privatsphäre in Sozialen Medien?

In Kürze

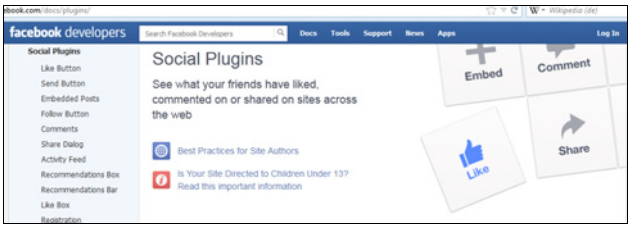
- Soziale Netzwerkseiten (SNS) wie z.B. Facebook oder Twitter sind heute allgegenwärtig. Sie entwickeln sich zunehmend zu Plattformen, die viele Dienste miteinander verknüpfen.
- SNS berühren in hohem Maße die Privatsphäre, da die darin abgebildeten Beziehungen, Inhalte und Interaktionen Individuen zugeordnet werden können.
- Das Recht auf informationelle Selbstbestimmung – also das Recht, selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen – ist in einer durch SNS geprägten Welt schwer durchsetzbar. Zusätzlich erschweren das die auf breite Vernetzung ausgelegten Nutzungsbedingungen und Geschäftsmodelle der Anbieter.
- Dies, sowie die jüngst bekannt gewordenen Überwachungsskandale, machen den dringenden Bedarf nach einer die Privatsphäre fördernden Gestaltung von SNS („Privacy-by-Design“) deutlich. Privacy-by-Design ist entscheidend, um das Vertrauen der NutzerInnen wiederherzustellen.

Worum geht es?

Soziale Netzwerkseiten (SNS) wurden seit der Gründung von Facebook 2004 zu einem allgegenwärtigen und ausgesprochen populären Phänomen im Internet. Sie ermöglichen auf relativ einfache Weise das Herstellen und Pflegen von sozialen Beziehungen. Die Nutzung reicht von rein privaten Zwecken (z.B. Austausch über Hobbies) bis zu beruflichen (z.B. Jobsuche, Marketing), von individuellen Kontakten bis zu Gruppenaktivitäten. SNS stellen dafür vielfältige Kommunikationsinstrumente zur Verfügung und unterstützen durch ausgeklügelte Algorithmen im Hintergrund die Vernetzung der NutzerInnen, z.B. durch automatisiertes Vorschlagen von Beiträgen anderer auf Basis bislang gezeigter Interessen.

Die Nutzung Sozialer Medien führt immer zum Austausch von personenbezogenen Daten und Informationen, wie etwa Fotos oder persönlichen Vorlieben – und das nicht nur zwischen den NutzerInnen, sondern auch mit dem SNS-Anbieter selbst. Diese Daten werden vom Anbieter nicht nur zur Optimierung der Anwendungen, sondern vor allem als Einnahmequelle (z.B. durch gezielte Werbung) verwendet. Diese Preisgabe von personenbezogenen Informationen empfinden die NutzerInnen nur teils als gewollt und hilfreich. Im Kern handelt es sich dabei um einen durch umfassende Speicherung, Verarbeitung und Verknüpfung meist erzwungenen, tiefen Eingriff in die Privatsphäre.

Der Wunsch nach selbstbestimmter Kontrolle, also darüber, wer, was, wann mit welchen personenbezogenen Daten tun können soll, steht somit in Konkurrenz zu den Geschäftsmodellen der SNS-Anbieter. Dabei haben die NutzerInnen praktisch keinen Einfluss auf die Nutzungsbedingungen. Wie das Beispiel Facebook zeigt, ist durch die automatischen Einstellungen mittlerweile praktisch alles öffentlich einsehbar, was nicht explizit als privat gekennzeichnet wird; manches lässt sich gar nicht mehr als privat eintragen.



Social Plugins in Facebook

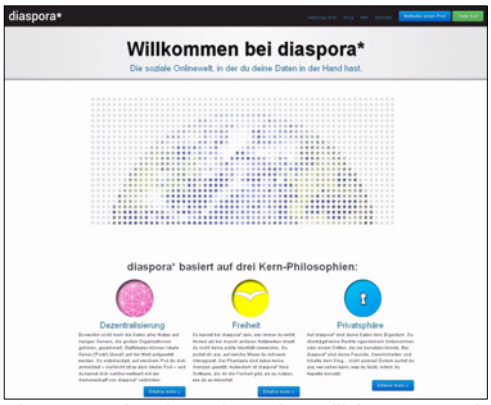
Weitere Herausforderungen für den Schutz der Privatsphäre ergeben sich aus der zunehmenden Verknüpfung von SNS mit anderen Online-Diensten. Zahlreiche sogenannte „Apps“ ermöglichen es Drittanbietern, etwa Spiele oder Waren anzubieten. Auch „Social Plugins“ stellen eine interaktive Brücke zwischen SNS und anderen Internetplattformen dar. So kann man etwa mit dem auf diversen Webseiten integrierten „Gefällt mir“-Button von Facebook externe Webinhalte teilen.

Eckdaten

Projekttitel:	Social Network Sites: Potentials, Impacts and Major Privacy Challenges
Projektteam:	Strauß, S., Nentwich, M., im Rahmen der European TA Group (ETAG)
Laufzeit:	04/2012 – 12/2013
Auftraggeber:	Europäisches Parlament/STOA

Analyse

Mehrere Studien haben ergeben, dass die meisten NutzerInnen von SNS große Mengen personenbezogener Daten teilen. Trotzdem ist für die Mehrheit der Schutz ihrer Privatsphäre wesentlich. Bewusstseinsfördernde Maßnahmen wie aufklärende Artikel sind zwar wichtig, angesichts der sehr eingeschränkten Möglichkeiten zur informationellen Selbstbestimmung reicht das aber nicht: Die Datenschutzeinstellungen in SNS sind privatsphären-gefährdend, intransparent, komplex zu bedienen und lassen in der Regel keinen umfassenden Schutz zu. Alternativen Angeboten wie dem privatsphären-freundlichen SNS Diaspora mangelt es bisher aber an Attraktivität.



Diaspora – ein privatsphärenfreundliches Netzwerk

Besonders aufgrund von Apps und Social Plugins greift der Schutz der direkt personen-bezogenen Daten zu kurz: Vor allem die durch diese Dienste gesammelten impliziten Daten, die nicht aktiv eingegeben werden, sondern automatisch durch die Nutzung entstehen, können zu einem aussagekräftigen Profil der NutzerInnen verdichtet werden. In diesem Zusammenhang spielt auch die rasante Entwicklung der Biometrie (z.B. Gesichtserkennung) und das weitere Anwachsen der mobilen Nutzung von SNS (samt Lokalisierung über GPS) eine gewichtige Rolle.

Ein individualisierter Zugang zum Schutz der Privatsphäre wird zwar prinzipiell durch verschiedene Instrumente (die etwa bestimmte Datenzugriffe abblocken) unterstützt. Ob und wie man ihn anwendet, hängt aber sehr von den unterschiedlichen Kenntnissen der einzelnen NutzerInnen ab. So entsteht eine spezielle Form der digitalen Spaltung, eine „Privacy Divide“. Eine Lösung ist der Ansatz „Privacy-by-Design“: Soziale Medien können auf technischer und organisatorischer Ebene so gestaltet werden, dass der Schutz der Privatsphäre der NutzerInnen von vornherein eingebaut ist, und nicht ausschließlich von deren Verhalten abhängt.

Was tun?

Soziale Netzwerkseiten gefährden die Privatsphäre, da die darin abgebildeten Beziehungen, Inhalte und Interaktionen Individuen zugeordnet werden können. Um diesem aufgrund neuerer Entwicklungen wachsenden Problem zu begegnen, reicht Bewusstseinsbildung allein nicht. Vielmehr wären zusätzliche Maßnahmen erforderlich:

- Privatsphärenschutz als Voreinstellung: Die privatsphärenfreundliche Gestaltung „Privacy-by -Design“ könnte die standardmäßig freie Zugänglichkeit aller Daten ablösen. Die Verschlüsselung von Inhalten und die Schaffung entsprechender Standards wären dafür wesentlich.
- Die Limitierung der Lebensdauer von Daten und die Möglichkeit zur permanenten Löschung würde die Informationelle Selbstbestimmung stärken.
- Wenn personenbezogene Daten prinzipiell dezentral gespeichert werden, könnten Informationen, die Personen identifizieren, nicht ohne weiteres außerhalb des ursprünglichen Kontexts miteinander verknüpft werden.
- Um die Einhaltung der Privacy-Standards besser zu prüfen, müssten die Datenschutzbehörden in ihrer Kontrollfunktion gestärkt und mit mehr Ressourcen ausgestattet werden.

Ein kritischer öffentlicher Diskurs zu Privatsphäre, Informationsfreiheit und Transparenz könnte das Vertrauen in SNS und andere Web-basierte Kommunikationsinfrastrukturen jedenfalls stärken.

Zum Weiterlesen

Strauß, S., Nentwich, M. (2013) Social Network Sites – Privacy and the blurring boundary between public and private spaces. Science and Public Policy, Bd. 40 (6), S. 1-9 (online first: 5/10/13).

Kontakt

PD Dr. Michael Nentwich

E-mail: tamail@oeaw.ac.at

Telefon: +43(1)51581-6582

IMPRESSUM: Medieninhaber: Österreichische Akademie der Wissenschaften; Juristische Person öffentlichen Rechts (BGBl. 569/1921 i.d.F. BGBl. I 130/2003); Dr. Ignaz Seipel-Platz 2, A-1010 Wien; Herausgeber: Institut für Technikfolgen-Abschätzung (ITA); Strohgasse 45/5, A-1030 Wien; http://www.oeaw.ac.at/ita | Erscheinungsweise: Die ITA-Dossiers erscheinen unregelmäßig und dienen der Veröffentlichung der Forschungsergebnisse des ITA. Die Dossiers werden in kleiner Auflage gedruckt und open access über das Portal „epub.oeaw“ zur Verfügung gestellt: http://epub.oeaw.ac.at/ita/ita-dossiers | ISSN: 2306-1960

ITA-Dossier Nr. 5, November 2013, http://epub.oeaw.ac.at/ita/ita-dossiers/ita-dossier005.pdf | Koautor: Strauß, S.