Mario Fischer und Tim Sebastian

»Facebook: Fluch, Segen oder Zeitbombe?

Die Diskussion um den Datenschutz im Web reißt nicht ab. Politik und Datenschützer vermuten auch bei Facebook diesbezüglich mögliche Gefahren. Offenbar ist die tatsächliche Brisanz aber noch nicht in die öffentliche Diskussion vorgedrungen, denn was Facebook über seine Nutzer preisgibt, ist teilweise erschreckend. Was für Online-Marketers ein Segen ist, könnte sich zur Zeitbombe für die Nutzer entwickeln.

Irgendwie wiederholt sich das immer wieder: Datenschützer warnen vor zu viel Preisgabe persönlicher Information im Web, und die Nutzer ignorieren das fröhlich und stellen alles über sich und oft auch ungefragt über ihr Umfeld in diverse Plattformen ein. Viele haben kein Problem damit, wenn die eigenen Freunde in Facebook lesen können, was man gerade tut oder welche Interessen man hat. Und alle anderen wird das der Vermutung nach sowieso nicht interessieren. Was soll also die ganze Aufregung? In der Ausgabe 29 des Nachrichtenmagazins „Der Focus“ hat die Bundesministerin Ilse Aigner in einem Interview gesagt, sie würde gerne wissen, welche Daten Facebook an Unternehmen weitergeben würde. Frau Aigner kann geholfen werden: Prinzipiell fast alle!

> „Ich möchte erfahren, welche Drittfirmen die Daten einsehen können und wie Werbekunden von den Profilen profitieren **Bundesministerin Ilse Aigner**

Das Brisante dabei ist wohl nicht, dass Besucher von Facebook die persönlichen Daten beim Betrachten der Seiten einsehen können. Erschreckend ist viel mehr, welcher Datenumfang und welche Detailtiefe elektronisch und damit problemlos speicher- und weiterverarbeitbar übermittelt werden. Die Datenschutzerklärung von Facebook ist deutlich länger als die amerikanische Verfassung. Und rechtlich steht sie dem Vernehmen nach trotzdem juristisch auf wackeligen Füßen. Das mag mit den zuweilen eigentümlichen Einstellungen des jungen Gründers, Marc Zuckerberg, zu tun haben, der mit seiner Idee aus seiner Sicht wohl die Welt des Mitmachwebs aus den Angeln gehoben hat. Bei seinen ersten Gehversuchen hatte er noch den Server der Uni gehackt und einfach alle Daten von Studentinnen publiziert und zum Voting aufgerufen. Das fanden wohl so viele seiner Kommilitonen richtig gut, und daraus ist letztlich der Wurf zu einer räumlich sehr viel größeren Version, nämlich Facebook, entstanden. Möglicherweise ist Zuckerberg, der bei der Gründung von Facebook ganze 19 Jahre alt war, auch heute noch der Meinung, alle von Nutzern eingestellten Daten gehören ausschließlich ihm oder seinem Unternehmen. Und daher könne man damit machen, was man möchte. Heute zählt er nach nur ein paar Jahren mit dieser Einstellung bereits zur Riege der Multimilliardäre. Es ist nur verständlich, dass ein so junger Mensch mit so extremem Erfolg zu der Einsicht gelangt, alles tun zu können, was er persönlich für richtig hält. Ob er die Idee zu Facebook tatsächlich selber hatte, oder ob einige seiner Prozessgegner recht haben, bleibt dahingestellt. Die nämlich werfen ihm Ideen- und Codeklau und auch Sabotage vor. Er hätte sich sogar in fremde Mailserver gehackt und gezielt Informationen manipuliert, um Gegner auszuschalten. Dazu hätte er teilweise sogar die internen Daten von deren Nutzeraccounts bei Facebook verwendet, um sich Zugang zu Mailkonten zu verschaffen und dort mitzulesen. Schließlich verwenden viele Menschen aus Bequemlichkeit nur ein Passwort für mehrere Dienste. Ob an einem Menschen ein solcher „Hy-

DIE AUTOREN

Dr. Mario Fischer ist Herausgeber von Website Boosting.

Tim Sebastian ist Online-Marketer und Head of Web-Development bei „Wir machen was mit Medien“, einer kreativen Kommunikationsagentur mit Fokus auf Neue Medien.

pererfolg“, den er schon als Jugendlicher eingeleitet hatte, spurlos vorübergehen kann? Wahrscheinlich nicht. Und wahrscheinlich ist das auch ein Teil des Charmes von Facebook – gleichzeitig aber auch etwas, über das man sich Sorgen machen muss. Denn in einem Interview mit Mike Arrington hat Zuckerberg verlauten lassen, dass er die Privatsphäre als ein für inzwischen veraltetes Konzept halte. Würde er Facebook noch einmal gründen, würde er alle Datenschutzeinstellungen von Anfang an auf öffentlich stellen (zu sehen unter *www.ustream.tv/recorded/3848950*).

Nachdem es viele Vermutungen darüber gibt, wie genau es Facebook mit dem Datenschutz nun tatsächlich nimmt, lohnt sicher ein genauer Blick. Und hier wird man gleich an mehreren Stellen fündig.

Welche Daten kann Facebook überhaupt sammeln?

Zunächst natürlich alle, die ein Nutzer dort einstellt. Das kann eine ganze Menge sein, wenn wirklich alle Felder ausgefüllt werden. Für die Profilierung, die Werbekunden danach vornehmen können, ist dies für ein genaues Targeting eine feine Sache. Nach diesen Profilangaben können Werbetreibende nämlich genau aussuchen, wen sie bewerben möchten (Abbildung 1).

Gleitend mit jeder Eingabe kann man dann erkennen, wie viele Nutzer man mit den verwendeten Filtern potenziell erreichen kann (Abbildung2 und Abbildung3).

Prinzipiell laufen aber bei Facebook noch sehr viel mehr und sehr viel interessantere Daten auf. Zum Beispiel zu einem gewissen Teil auch, wo angemeldete Nutzer surfen bzw. welche Webseiten sie aufrufen. Dies hört sich zunächst unglaublich an, funktioniert aber, weil sich viele Seitenbetreiber zumindest in dieser Hinsicht als Steigbügelhalter für Facebook nutzen lassen. Um an dem Hype „Social Networks“ entsprechen-

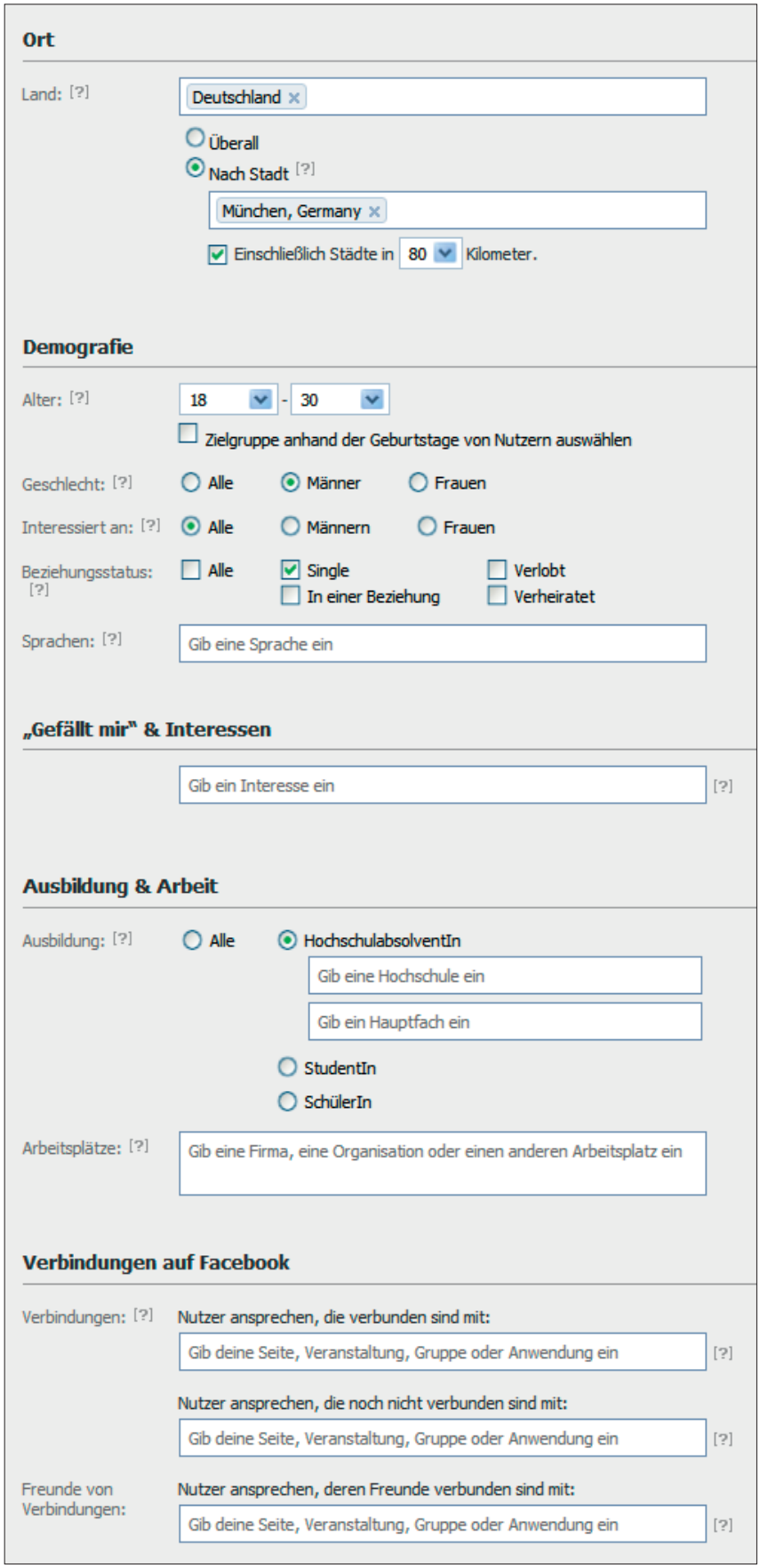

Abbildung 1: Die Targeting-Möglichkeiten für Werbung bei Facebook

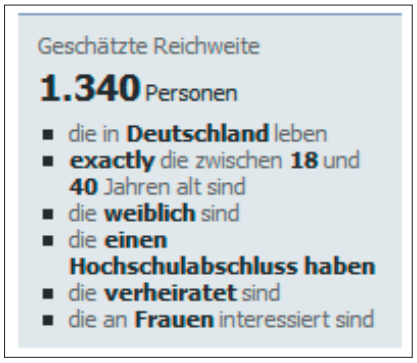

Abbildung 2: Junge, gebildete Frauen, die an Frauen interessiert - und verheiratet sind

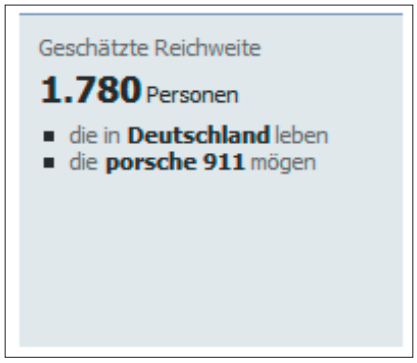

Abbildung 3: Bei wem wäre Werbung für den 911er Porsche gut platziert?

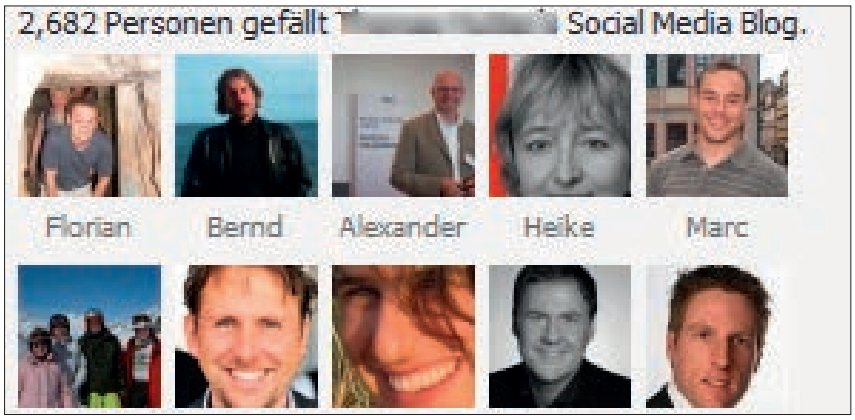

Abbildung 5 Vollautomatisch Freunde des Besuchers anzeigen lassen

den Anteil zu haben, binden nämlich immer mehr Seitenbesitzer den „Gefällt mir“-(Like this)-Button von Facebook auf ihre Seiten ein.

Man möchte seine Besucher dazu bringen, durch das Drücken des Buttons kundzutun, dass man dieses Unternehmen bzw. diese Webseite gut findet. Das kann dann wiederum jeder sehen. Wenn meine Freunde etwas mögen, kann es vielleicht nicht so verkehrt für mich sein. Das ist vom Ansatz her auch gut so und schafft Vertrauen (siehe den Beitrag von Tim Ash in dieser Ausgabe). Geht der Seitenbetreiber in puncto „Vertrauensbildung“ noch ein Stück weiter, kann er per Code von Facebook sogar automatisiert Bilder der Freunde des Besuchers einbinden, wie in dem Beispiel eines Social Media Blogs in Abbildung 5 zu sehen ist.

Wer bis hierher aufmerksam mitgedacht hat, bei dem gehen jetzt wahrscheinlich die Alarmglocken an. Woher weiß die Website XYZ, welche Freunde ich auf Facebook habe? Ganz einfach: Durch das Einbinden eines Facebook-Skripts in die Website XYZ bekommt die Infrastruktur von Facebook den Besuch übermittelt, und wenn ein Nutzer vorher bei Facebook angemeldet war oder mit seinem Browser ständig eingeloggt bleibt (also keinen Benutzernamen und Passwort beim Aufrufen von Facebook eingeben muss), erkennt Facebook ihn persönlich an dem gesetzten Cookie.

```
<iframe src="http://www.facebook.com/plugins/like.php?href=www.website-XYZ.com&amp;layout=standard&amp;show_faces=true&amp;width=450&amp;action=like&amp;colorscheme=light&amp;height=80" scrolling="no" frameborder="0" style="border:none; overflow:hidden; width:450px; height:80px;" allowTransparency="true"></iframe>
```

Damit „weiß“ Facebook von jedem Seitenbesuch von mir, solange ich in derselben Browsersession oder eben dauerhaft eingeloggt bin und eine Seite diesen „Gefällt mir“-Button eingebunden hat. Wer sich mit diesen technischen Details nicht auskennt, den mag vielleicht überzeugen, dass Facebook ja gezielt Bilder von Freunden auf jeder beliebigen Webseite anzeigen kann (siehe Abbildung 5), die gar nicht zu Facebook gehört. Man muss bei Facebook also rekonstruieren können, wann und welcher Nutzer sich auf Website A tummelt. Damit ist Facebook technisch dazu in der Lage, von allen 500 Mio. Nutzern Bewegungsprofile bzw. Webseitenbesuche auf Seiten mit dem besagten Button aufzuzeichnen. Dazu genügt es, wenn ein Websitebetreiber den Facebook-Code einbindet und sich somit in gewisser Weise zum Steigbügelhalter dieser bedenklichen Datensammlung macht. Dabei reicht wohlgemerkt das bloße Aufrufen einer solchen Seite mit einem Facebook-Button. Er muss noch nicht einmal gedrückt werden.

Besonders pikant wird diese Betrachtung, wenn man berücksichtigt, dass wahrscheinlich die meisten Facebook-Nutzer dort ihre wahre Identität hinterlegt haben – wozu sie laut Facebook sogar verpflichtet sind. Das Anlegen von nicht realen Personen oder fal-

> Gegen die personalisierten Profildatenbanken von Facebook erscheint Google wie ein pubertierender Schuljunge, der anonyme Liebesbriefchen in einem Setzkasten sammelt

schen persönlichen Informationen ist nach den Richtlinien nämlich nicht erlaubt. Facebook kann also zu jedem Nutzerprofil zumindest teilweise dessen Webseitenaufrufe aufzeichnen. Ob dies tatsächlich gemacht wird, ist nicht bekannt, aber im Hinblick auf die geäußerten Einstellungen des Gründers darf dies zumindest vermutet werden. Umso erstaunlicher ist es, dass deutsche Datenschützer hier diesmal nicht zum Sturm blasen, obwohl dies mehr als gerechtfertigt wäre. Denn anders als das US-amerikanische Unternehmen Facebook unterliegen die verantwortlichen Webmaster aus Deutschland natürlich deutschem Recht. Prinzipiell unterstützen diese Webmaster – ohne den Sitebesucher vorab zu fragen oder ihn darauf hinzuweisen – das schwer kontrollierbare Speichern echter, personenbezogener Daten für einen ausländischen Anbieter. Gegen den Datenpool, den Facebook damit potenziell aufbauen kann, erscheinen alle aktuellen Diskussionen um die Speicherung von IP-Adressen oder Google Street View im Vergleich wie der Streit von Schülern, die sich gegenseitig das Pausenbrot aus der Hand schlagen wollen. Die Speicherung personenbezogener Daten ist in Deutschland bekanntermaßen zustimmungspflichtig. Da das vorherige rechtssichere Einholen dieser Zustimmung beim „Betreten" einer Website illusorisch erscheint, würde nur der Verzicht auf die Einbindung von Facebook-Skripten Abhilfe bringen. Eine verlässliche juristische Bewertung dieses Sachverhalts steht noch aus, aber vieles aus vergleichbaren Fällen deutet darauf hin, dass sich hier ein nicht zu unterschätzendes Problem für unbedarft handelnde Webmaster auftun könnte. Ebenfalls zu klären wäre, ob das Durcharbeiten der umfassenden Datenschutzrichtlinien und die Erklärung der Rechte und Pflichten mit insgesamt etwa 33 Seiten aus juristischer Sicht zumutbar und für den normalen Nutzer überhaupt zu verstehen sind. Es ist in der Tat daher nicht

> „Die Einbindung des "Gefällt mir"-Buttons in Deutschland ist meiner Einschätzung nach datenschutzwidrig und somit illegal.
> **Dr. Martin Bahr, Rechtsanwalt**

so, dass Facebook die gesammelten Daten klammheimlich weitergibt. Natürlich kann man auch argumentieren, dass man ja keinen Account bei Facebook anlegen müsse, wenn man diese Richtlinien nicht versteht oder selbst schuld wäre, weil man sie nicht genau durchgelesen hat. In der Praxis wird es vermutlich wohl doch eher so sein, dass sich die meisten Nutzer dieser umfassenden Rechte (und Pflichten) tatsächlich nicht bewusst sein dürften, die sich Facebook bezüglich der Datenspeicherung und -weitergabe selbst einräumt.

Kann man als Dritter an die Daten von Facebook-Nutzern kommen?

Bisher ging es um Daten, die auf den Servern von Facebook liegen. Die Profildaten kann man zwar teilweise auch auf den entsprechenden Nutzerseiten einsehen, aber für echte Datensammler ist dies sicherlich ein zu mühsamer Weg.

Durch die recht offen gestalteten Schnittstellen (API) von Facebook gibt es aber noch einen anderen, sehr viel bequemeren Weg: die Erstellung einer als nützlich erachteten Facebook-Applikation (App). Das sind Anwendungen, die man selbst nach den Richtlinien von Facebook erstellen kann und die dann über Facebook allen Nutzern zur Verfügung stehen. Das wohl bekannteste App ist Farmville – ein Spiel, bei dem man online Felder bewirtschaftet und dabei mit anderen Facebook-Nutzern interagieren kann, sofern die es ebenfalls nutzen. Facebook ist voll von diesen Apps, und in der Regel sorgen die Entwickler der Apps dafür, dass sie eine schnelle Verbreitung finden. Nutzt ein Facebook-Mitglied eine solche App, wird oft automatisch und ohne Zutun des Nutzers eine Meldung an alle Freunde dieses Mitglieds mit Einladungen verschickt. Über die offenen Programmierschnitt-

Welche Daten bekommt man prinzipiell via Facebook übertragen?		
ID (des Profils)	Geschlechtsinteressen	Bücher
Name	Beziehungssuche	Filme
Vorname	Beziehungsstatus	Fernsehen
Nachname	Religion	Alle „like" Votings
Link (des Profils)	Politische Einstellung	Gruppenzugehörigkeiten
About (was man über sich selbst schreibt)	Verifizierter Account (per SMS)	Alben
Geburtstag	Weitere Freitextangaben	Videos
Arbeitsstätte	Zeitzone	Notizen
Bildung/Schulen	Newsfeed des Nutzers	Events
E-Mail	Linkadresse zum Bild des Nutzers	Feed
Website	Aktivitäten	Bilder
Wohnort	Interessensgebiete	Status-Historie
Wo der Nutzer gerade ist (Location)	Musikinteressen	Alle je geposteten Links
Geschlecht		

Abbildung 6: Ein beispielhafter Datenstream. Wie war wohl der Urlaub von K auf Santorini?

stellen (API) von Facebook wird dem jeweiligen App dann auch ein recht umfassender Datenstream über die Person übermittelt, welche das App genutzt hat. Je nach den gewählten Einstellungen des Facebook-Mitglieds und was er der Applikation erlaubt werden fast alle Daten von ihm an den Ersteller der App übermittelt. Und nicht nur diese. Auch die Daten aller Freunde des Nutzers werden je nach den gewählten Einstellungen ebenfalls gleich mit übertragen. Welche Daten man prinzipiell dabei erhalten kann, zeigt Tabelle 1.

Diese Daten werden wohlgemerkt an den (fremden) Server des App-Erstellers geschickt und können dort gespeichert werden. In den Richtlinien von Facebook steht zwar, dass man diese Daten maximal bis zu einem Tag speichern dürfe, aber es ist natürlich längst nicht sicher, dass sich alle Anbieter daran halten. Für Datensammler öffnet sich hier offenbar ein wahres Eldorado. Je nachdem, wie nützlich die App erscheint, können durch den automatischen „Weitersagen"-Effekt schnell so viele Daten zusammenkommen, dass der von Facebook gelieferte Datenstream mit normalen Bordmitteln und ohne Hochleistungshardware und schneller Internetverbindung gar nicht mehr übertrag- und verarbeitbar wird. Schließlich hat jeder Facebook-Nutzer im Durchschnitt etwa 130 Freunde. Da kommt schnell eine ganze Menge zusammen. In Abbildung 6 ist ein anonymisierter Datenstream beispielhaft dargestellt, wie ihn Facebook zur Verfügung stellt. Dabei können unter Umständen je nach Nutzerverhalten auch Bewegungsprofile aus dem realen Leben und detaillierte Interessengebiete ausgewertet werden (siehe Abbildung 7).

Vielleicht mag man sich ab und zu wundern, warum Entwickler so viel Zeit und Energie in die Entwicklung kostenlos nutzbarer Apps stecken. Möglicherweise besteht der Hintergrund dieses vermuteten Altruismus in Einzelfällen auch in der Sammlung von Nutzerdaten. Da ja auch die Profilbilder von Nutzern mit übertragen werden, könnten hier personalisierte Datenbanken bzw. „Steckbriefe" aufgebaut werden, die eigentlich Datenschützern in allen Ländern ihre bisherigen Bemühungen wie das Entfernen weniger Ameisen aus einem wuselnden Haufen vorkommen müssen. Damit soll nicht der Eindruck entstehen, dass alle App-Ersteller finstere Absichten hätten. Im Gegenteil – dürften die meisten wohl sicherlich die Nützlichkeit und/oder die Teilnahme an dem aufkommenden „Social Web"-Hype im Auge haben. Und bei einigen Entwicklern wird vielleicht auch bereits die vielen für alle sichtbaren „mag ich"-Votings Entlohnung genug sein. Fremde Menschen mögen etwas, in das man als Entwickler unter Umständen viel Mühe und Fleiß gesteckt hat. Facebook hat mit einem entsprechenden Button („Anwendung melden") auch dafür Sorge getragen, dass offensichtlicher Missbrauch bei Apps per Mausklick gemeldet werden kann. Leider kann man in der Regel nicht erkennen, ob eine App von den umfassenden Datenübertragungsmöglichkeiten tatsächlich Gebrauch macht und welche von den Apps denn nun wirklich „böse" sind bzw. welche den alleinigen Zweck des Datensammelns haben. Das stellt sich wahrscheinlich – wenn überhaupt – erst viel zu spät heraus. Facebook hat hier selbstverständlich juristisch vorgesorgt, indem man Anbietern von Applikationen per Richtlinien u. a. vorschreibt, dass sie nur die Daten anfordern und speichern dürfen, die sie für die Applikation selber benötigen. Ebenso verpflichten sich alle Entwickler automatisch per Richtlinie, Daten auf Verlangen von Nutzern zu löschen. In der Praxis dürfte dies schwer durchzusetzen und vor allem zu kontrollieren sein, auch von Facebook

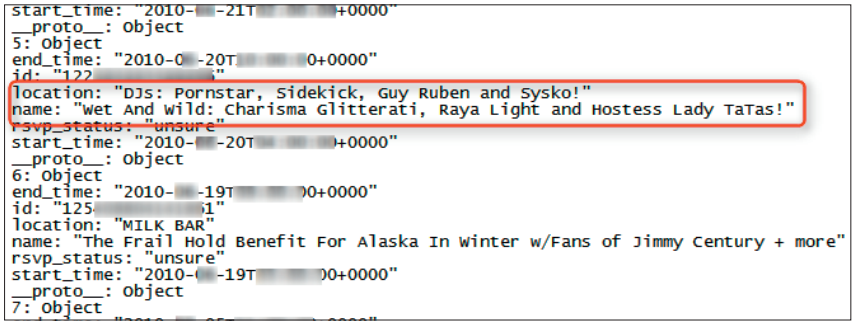

Abbildung 7: Ob K. wohl die Einladung mit DJ Pornstar in San Francisco angenommen hat?

Abbildung 9 Ein Freund schlägt Dir was vor...

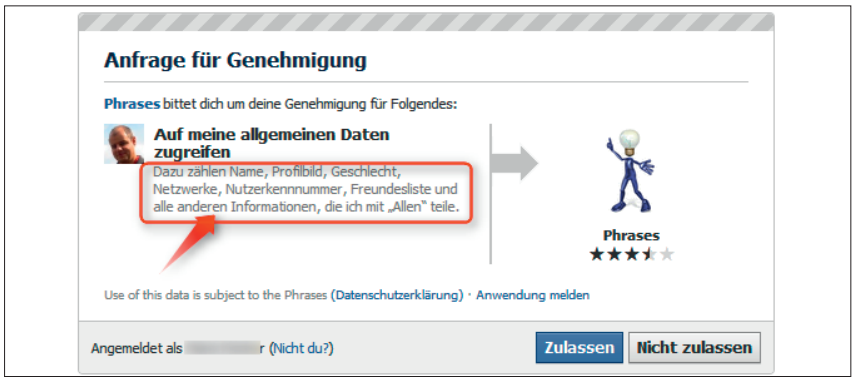

Abbildung 10 Sicherheitsabfrage: Darf diese Anwendung auf das eigene Profil und alle meine Freunde zugreifen?

selber nicht. Per Datenschutzrichtlinie und der im Impressum hinterlegten „Erklärung der Rechte und Pflichten" wird also im Prinzip jeglicher Missbrauch umfassend untersagt – und trotzdem lässt er sich technisch recht leicht realisieren.

Vor Kurzem hat ein namhaftes Unternehmen aus der Kosmetikbranche bekannt gegeben, dass sie ihre eigene Homepage aufgeben und sich ausschließlich auf die Fanpage bei Facebook konzentrieren möchte. Ob eine solche Entscheidung strategisch wirklich sinnvoll ist, kann man ohne Kenntnis der Beweggründe sicher nicht beurteilen. Ob sie rechtlich aus Sicht der deutschen Datenschutzgesetze spannend ist, kann wohl klar mit einem Ja beantwortet werden.

Tue Böses und rede eben nicht darüber

„Chantal Mustermann möchte mit dir auf Facebook befreundet sein." Die hohe Anzahl an „Freunden" bei den meisten Facebook-Nutzern resultiert wohl zu einem gewissen Grad auch daher, weil viele solche Freundschaftsanfragen be-

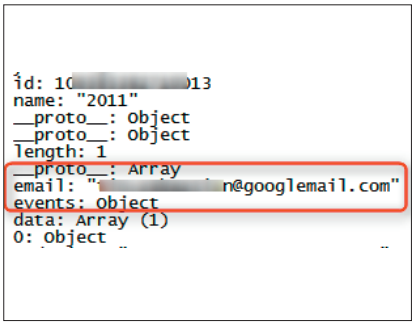

Abbildung 8: Auch E-Mail-Adressen können an Applikationen übertragen und damit unter Umständen auf fremden Servern gespeichert werden.

jahen – auch wenn sie die anfragende Person nicht so gut oder gar nicht kennen. Datensammler könnten nun auf die Idee kommen, ein gefaktes, also unechtes Profil mit einem hübschen Frauen- und/oder Männergesicht einzustellen und mit maschinellen Tricks (per Bot) möglichst viele Freunde einzusammeln. Die Erfahrung zeigt, dass dieses Einsammeln mit attraktiven Gesichtern recht gut klappt. Hübsche Menschen „kennt" fast jeder gerne. Im zweiten Schritt entwickelt man nun eine Applikation für Facebook und installiert diese nur mit diesem bzw. diesen unechten Account(s). Je nach Datenschutzeinstellungen der Freunde werden nun automatisch die verfügbaren Daten dieser Freunde mit übertragen. Es genügt also, wenn nur ein gar nicht real existierender Facebook-Nutzer einer Applikation zustimmt, und schon gelangt man an Hunderte oder Tausende Daten von anderen Facebook-Nutzern (eben der Freunde). Gelänge es nun noch, diese per Nachricht oder Mail ebenfalls zu Nutzern der eigenen Applikation zu machen, tritt schnell der berühmte Schachbrett- oder Lawineneffekt ein: Mit jedem neuen Nutzer erhöht sich die Anzahl der möglichen neuen Datensätze statistisch um weitere 130 (das ist wie erwähnt die durchschnittliche Anzahl an Freunden, die jeder Facebook-Nutzer hat).

Geht man davon aus, dass von denen jeweils nur jeder Zehnte von 130 die vom „Freund" empfohlene Applikation

> Eine geschickt platzierte Applikation könnte theoretisch bereits nach einigen Tagen auf einen Datenstream von über5 Mio. Facebook-Nutzern zugreifen

auch tatsächlich nutzt, erreicht man damit rein rechnerisch in der fünften Stufe bereits über 5 Mio. Accounts bzw. kann sich deren Daten übertragen lassen. Eine Stufe weiter wären es dann schon knapp 70 Mio. Da die Verbreitungsgeschwindigkeit von der tatsächlich erreichten Nutzergruppe abhängt sowie von deren Datenschutzeinstellungen, ist dies allerdings nur ein theoretisches, aber durchaus erschreckendes Rechenspiel. Bleibt noch darauf hinzuweisen, dass Applikationen durchaus mehr persönliche Daten bekommen können, als in den Datenschutzeinstellungen hinterlegt ist. Das ist dann der Fall, wenn der Benutzer dies bei der Installation zulässt, weil er die Applikation z. B. unbedingt haben möchte oder den Hinweis (Abbildung 10) übersieht und trotzdem zustimmt.

Und als wäre das alles datenschutzrechtlich noch nicht bedenklich genug, gibt es noch eine weitere Möglichkeit für den Ersteller einer App, aktiv weitere Profilierungsinformationen zu sammeln. Technisch besteht nämlich die Möglichkeit, eingeloggte Facebook-Nutzer, welche die erstellte App nutzen, auch auf anderen Websites zu identifizieren.

Da sich Apps per App-ID, API-Key und Sicherheitsschlüssel bei Facebook authentifizieren und anschließend per IFrame in Facebook eingebunden werden, ist es technisch gesehen irrelevant, ob ein Besucher sich nun auf Facebook befindet oder auf der eigenen Website. Solange der Host, der für die App registriert ist, derselbe ist, kann jederzeit auf die von Facebook angebotene API zugegriffen werden. Besucht also jemand, der das eigene App einmal genutzt hat und aktiv bei Facebook eingeloggt ist, die eigene Website – dann könnte man ihn tatsächlich über seine Facebook-ID* identifizieren und unter seinem Profil

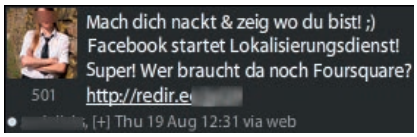

Abbildung 11: Diese Twitterin hat wohl noch Bedenken gegen Facebook Places.

den Sitebesuch hinzufügen. Man könnte ihn dann auf einer dynamisch erzeugten Seite sogar per Namen und mit eigenem Bild begrüßen. Ein entsprechender Test, dass Personen tatsächlich namentlich auf der eigenen Website über die Schnittstelle zu Facebook erkannt werden können, liegt Website Boosting vor.

Einigen App-Programmierern erlaubt Facebook offenbar sogar, auf die persönlichen Mailboxen von Nutzern zuzugreifen, falls diese die App benutzen. Die Funktion „read_mailbox“ wird beschrieben mit „Provides the ability to read from a user's Facebook Inbox. You must request to be whitelisted before you can prompt for this permission.“ Für diese Postfach-API (O-Ton Facebook: „Mit der Postfach-API kannst du auf die Nachrichten von Nutzern zugreifen, wenn sie deiner Anwendung erweiterte Genehmigungen geben.“) muss man sich also bei Facebook erst über ein Bewerbungsformular die Erlaubnis einholen (www.facebook.com/help/contact.php?show_form=inbox_api_whitelist). Nach welchen Kriterien Facebook App-Entwicklern dann tatsächlich Zugriff auf die persönlichen Mails der Nutzer erlaubt, wird nicht weiter erläutert.

Natürlich darf man bei all diesen Betrachtungen nicht aus den Augen verlieren, dass Facebook aufgrund der breiten und massiven Kritik an den Datenschutzbestimmungen den Nutzern mittlerweile eine recht umfangreiche Kontrollmöglichkeit eingeräumt hat. Darüber lässt sich steuern, welche Daten wem zur Verfügung gestellt werden. Insofern liegt der größte Teil des schwarzen Datenschutz-Peters beim Nutzer selbst. Man kann jedoch mit hoher Wahrscheinlichkeit auch hier davon ausgehen, dass den wenigsten Nutzern bewusst sein dürfte, dass eben nicht nur Freunde und Freunde von Freunden die eigenen Profildaten, Bilder, Nachrichten etc. auf den Facebook-Seiten selber einsehen können, sondern dass diese Daten eben möglicherweise auch maschinell verarbeitbar Dritten zur Verfügung gestellt werden. Facebook macht es sich hier vielleicht etwas zu leicht, denn man verbittet sich einfach jeglichen Missbrauch in den Richtlinien. Wie es zu bewerten ist, dass dieser trotzdem recht einfach zu bewerkstelligen ist, bleibt dem Einzelnen selbst überlassen. Dazu kommt der eigentlich untragbare Umstand, dass man beim Anlegen eines neuen Profils diesen Richtlinien weder aktiv mit einer Hakensetzung zustimmen muss, noch diese während der Registierung per Link zur Verfügung gestellt und damit überhaupt zur Kenntnis bekommt. Ob sie damit überhaupt in Deutschland Rechtskraft erlangen, ist zweifelhaft.

TIPP:

Welche Daten Facebook an wen übermittelt, kann man unter „Konto“/Privatsphäre-Einstellungen festlegen. Bei „Inhalte auf Facebook teilen“ sollte man dazu die benutzerdefinierten Einstellungen wählen und einzeln aktivieren oder deaktivieren, wer was zu sehen bekommt. Wer nicht an der geografischen Verfolgung teilnehmen möchte, stellt dort am besten unter „Orte, die ich besuche“ die Option „Nur ich“ ein und deaktiviert das Kästchen bei „‚Mich‘ im ‚Personen, die jetzt hier sind‘-Abschnitt anzeigen, nachdem ich angegeben habe, wo ich mich befinde“. Zusätzlich empfiehlt es sich, die Option „Freunde können angeben, dass ich mich an einem Ort befinde“ zu sperren.

* siehe Glossar Seite 96-98

Abbildung 12: Eigene E-Mail-Kontakte bei Facebook abliefern

Abbildung 13: Facebook nimmt auch gerne persönliche Messenger-Kontakte der Nutzer entgegen.

Wo bist Du und was machst Du gerade?

Kurz vor Redaktionsschluss gab Facebook bekannt, in den USA einen Lokalisierungsdienst („Places“) zu starten, der bald auch nach Deutschland kommt. Dabei können Nutzer ihren realen Standort z. B. via Mobiltelefon bekannt geben und dem Vernehmen nach auch Freunde markieren (taggen), die selber kein Smartphone besitzen. Somit kann man seine Freunde gleich mit „einchecken“. Laut Facebook müssen die Freunde dem aber zustimmen. Falls diese lokalisierten Daten auch über die offenen Schnittstellen übertragen werden – wovon man nach dem bisherigen Datenschutzgebaren von Facebook durchaus ausgehen darf –, schwimmt zukünftig auf der Datensammlung noch ein ganz anderes, ein geografisches Fettauge. Gerade jüngeren Menschen ist es ja durchaus willkommen, wenn deren Freunde sehen können, wo man gerade ist und was man tut. Das ist schließlich der Sinn eines sozialen Netzwerkes. Aber dass diese teilweise doch recht intimen Daten, zusammen mit allen anderen Profildaten, Bildern, Nachrichten etc. und nun neu auch Aufenthaltsorte, eben möglicherweise auch an in der Regel unbekannte Dritte und deren Server zur unkontrollierbaren Speicherung übertragen werden, ist wohl den meisten so nicht bewusst. Insofern hat Facebook wohl weitgehend unbemerkt das geschafft, das Medien und Politiker Google oft aus technischer Unkenntnis heraus zu Unrecht ankreiden: den wertvollsten Pool an wirklich personalisierten Daten aufzubauen, den das Web 2.0 zu bieten hat.

Und täglich kommen zu den 500 Mio. Profilen weitere dazu. Denn Facebook macht es seinen Nutzern recht einfach, weitere Freunde zu finden. Dazu fordert man den Nutzer auf, den E-Mail-Account durchstöbern zu lassen oder auch die Chatlisten. Ob die so erlangten Daten vertraulich behandelt werden und welche der Daten durch den Vollzugriff auf ein Mailkonto tatsächlich bei Facebook gespeichert werden, weiß nur Facebook selbst. Prinzipiell wäre es möglich, nach Preisgabe von Mailkonto und Passwort alle je geschriebenen und erhaltenen Mails abzurufen (Abbildung 12).

INFO:

Möchten Sie wissen, mit wem ein Facebook-Nutzer befreundet ist? Facebook gibt dies völlig ohne Zustimmung dieses Nutzers freimütig preis. Dazu müsste man nur einen neuen Account anlegen (was allerdings in den Richtlinien untersagt ist, denn jeder darf nur einen Account haben und darin keine falschen Angaben machen) und der entsprechenden Person eine Freundschaftsanfrage schicken. Diese reine Anfrage genügt Facebook bereits, um sofort dessen Freunde mit Namen und Bild als potenzielle eigene Freunde freimütig abzuliefern! Für das Social Networking sicher nützlich, aber aus Datenschutzgründen ein Albtraum.

Komm doch mal vorbei!

Für Unternehmen kann sich hier aber durchaus ein sehr nützlicher Werbekanal ergeben. Wer sich in der Nähe eines Geschäftes bzw. einer Filiale aufhält, kann mit Sonderangeboten oder speziellen Rabatten direkt in den Laden gelockt werden. Falls sich hierfür noch kombiniert die Profilfilter nutzen lassen, würde ein mächtiges Werbeinstrument nicht nur für große, sondern gerade auch für kleine, lokale Unternehmen entstehen: „Alle Facebook-Nutzer aus Deutschland, die älter als 30 Jahre alt sind, aber nicht mehr studieren, männlich sind und in einer Beziehung leben, verlobt oder verheiratet sind und sich im Umkreis von 2 km um meinen Blumenladen befinden, bekommen 15 % Rabatt auf rote Rosensträuße“ – Werbetext: „Sie liebt Dich – Du sie auch? Baccararosen mit 15 % Liebesnachlass gleich hier um die Ecke!“ Jetzt entsteht aber möglicherweise der größte Gewissenskonflikt überhaupt: Soll man gegenüber der Frau oder Freundin zugeben, dass letztlich Facebook einen an diesen Liebesbeweis erinnert hat oder sich der Diskussion stellen, ob und warum man denn ein schlechtes Gewissen hat…¶

BLOG

Was ist Ihre Meinung zu Facebook? Diskutieren Sie mit uns unter…
» www.websiteboosting.com/blog