Datenschutz auf Facebook: Wem gehören meine Daten?

Autoren: Valie Djordjevic, David Pachali, Alexander Wragge

Soziale Netzwerke sammeln Daten – so weit, so bekannt. Doch was Facebook weiß, darüber gibt es oft Gerüchte und Halbwissen. Welche Daten sammelt Facebook, wie werden sie verwendet und wie können Nutzer darauf Einfluss nehmen?

Facebook polarisiert. Auf der einen Seite lässt sich der Nutzen kaum bestreiten: Freunde und Bekannte tauschen sich über die Plattform aus, teilen Fotos, Videos und Texte, posten und diskutieren. Selbst mit Freunden, die auf der anderen Seite des Erdballs leben, ermöglicht Facebook den täglichen, unkomplizierten Kontakt. Auf der anderen Seite sorgen sich viele Nutzer, dass sie mit ihren Daten für den kostenlosen Dienst bezahlen.

Facebook steht dabei mit seinen Praktiken nicht allein da. Auch andere soziale Netzwerke und Internetdienste sammeln auf ähnliche Weise Daten. Grundsätzlich werden im Netz sehr viele Nutzerdaten gesammelt, nicht nur von Facebook. Webtracking etwa, das Nachverfolgen des individuellen Surfverhaltens, ist keine Erfindung von Facebook. Sehr viele Webseiten nutzen entsprechende Techniken, um zu verfolgen, wo sich Nutzer bewegen, was sie anklicken, was sie interessiert und so weiter. Gerade Webtracking ist unter Datenschutz-Gesichtspunkten schnell problematisch, vielen Nutzern aber nur ansatzweise bekannt. Da Facebook aber das meistgenutzte Netzwerk weltweit ist, schauen wir es uns hier genauer an.

Das Geschäftsmodell von Facebook oder: Wozu verwendet Facebook die Daten?

Zunächst ist festzuhalten: Facebook funktioniert nicht wie eine weltumspannende Detektei, die Dritten (zum Beispiel anderen Unternehmen) einfach so über eine Person Auskunft gibt – das wäre rechtlich kaum möglich. Den Schatz der Nutzerprofile behält das Unternehmen aus eigenem Interesse weitestgehend für sich. Facebooks Geschäftsmodell basiert im Wesentlichen darauf, eine Plattform für personalisierte Werbung zu sein. Je besser Facebook seine Mitglieder kennt, desto besser kann es Firmen Anzeigen verkaufen, die zielgenau auf den Bildschirmen der potenziellen Kunden landen.

Folgt man den offiziellen Statements von Facebook, dann dient die umfangreiche Datenerfassung allein zwei mehr oder minder kommerziellen Zwecken: Erstens dem **Betrieb und der Verbesserung des Dienstes** – und damit der Nutzerbindung und der Gewinnung neuer Mitglieder – und zweitens der **Optimierung der Anzeigenschaltung**. Dabei gibt Facebook normalerweise ohne Zustimmung der Nutzer keine personenbezogenen

Daten an Dritte weiter (zu den Ausnahmen siehe weiter unten im Text). Es nutzt die gesammelten Daten in erster Linie, um Erlöse über Werbung zu erzielen, sortiert die Nutzer in zahlreiche Zielgruppen ein und schaltet die entsprechenden Anzeigen.

Die Zielgruppe solcher Anzeigen kann prinzipiell sehr kleinteilig definiert werden, zum Beispiel verheiratete Akademikerinnen in Berlin mit einem Monatseinkommen über 5.000 Euro, die Wohneigentum besitzen, in den letzten vier Monaten beim Onlinehändler Schuhe gekauft haben und in deren Freundeskreis ein Geburtstag ansteht. Dadurch, dass zum Beispiel der Händler ebenfalls Facebook-Funktionen auf seiner Website eingebunden hat, weiß Facebook bereits über die Einkaufsgewohnheiten Bescheid. Rund 1.300 Merkmale für Werbeschaltungen, die Facebook seinen Nutzern zuweist, sind bekannt.

Wenn Dritte Zugang haben wollen

Zu den Fällen, in denen Facebook Daten über Nutzer an Dritte weitergibt, gehören in erster Linie Zwecke der **Strafverfolgung**. Dazu dürfen Daten per Gerichtsbeschluss an Ermittlungsbehörden herausgegeben werden. In Deutschland erhielt Facebook eigenen Angaben zufolge im ersten Halbjahr 2016 rund 3.600 solcher Anfragen, welche rund 4.500 Nutzerkonten betrafen. In rund der Hälfte der Fälle gibt Facebook an, entsprechende Datensätze produziert zu haben. In manchen Ländern können Unternehmen wie Facebook auch zur Zusammenarbeit mit Geheimdiensten gezwungen werden, ohne dass sie darüber reden dürfen – so in den USA, wie spätestens seit den Enthüllungen von Edward Snowden bekannt ist.

Auch andere Stellen zeigen sich immer wieder interessiert, Daten von Facebook zu nutzen. So hat die Wirtschaftsauskunftei Schufa 2012 geprüft, inwieweit sie Daten aus sozialen Medien nutzen kann, um die **Kreditwürdigkeit** einer Person zu beurteilen. Nach heftiger Kritik von Datenschützern wurde das Projekt später fallen gelassen. Andere Firmen verfolgen ähnliche Ansätze unterdessen weiter, etwa das Hamburger Unternehmen Kreditech. Weitere Unternehmen hätten gerne einen Zugang zu Facebook-Daten, scheiterten damit aber bislang: So plante etwa der britische Versicherer Admiral, Kfz-Nutzer mit günstigeren Tarifen zu locken, wenn sie Daten ihres Facebook-Profils offenlegen. In diesem Fall wandte sich Facebook selbst gegen die Pläne.

Nach der firmeneigenen „Plattform-Richtlinie“ sollen Nutzerdaten nicht verwendet werden, um Entscheidungen über eine „Berechtigung, Eignung oder Auswahl“ zu treffen, beispielsweise im Rahmen einer Kreditvergabe (Stand 2/2017). Die Richtlinie wendet sich allerdings in erster Linie an Dritte, die Anwendungen für Facebook entwickeln. Sie schließt also nicht aus, dass Facebook selbst in Zukunft entsprechende Pläne fassen

oder Kooperationen starten könnte. Das Unternehmen verfügt auch bereits über Patentanmeldungen, die es zu diesem Zweck nutzen könnte. Solche Nutzungen würden gleichwohl sehr schnell in Konflikt mit deutschen und europäischen Datenschutzgrundsätzen geraten.

Grundsätzlich müssen sich Nutzer also entscheiden, inwieweit sie Facebook vertrauen, wenn sie dem Unternehmen ihre Daten preisgeben. Das Problem: Es ist gar nicht so einfach, eine informierte Entscheidung darüber zu treffen, ob man das will. Mögliche Folgen in der Zukunft lassen sich nur schwer abwägen. Und je stärker der eigene Bekanntenkreis eine bestimmte Plattform nutzt, desto schwerer lässt sich zugleich darauf verzichten. Ein anderes Problem besteht darin, dass Facebook bei der Weiterentwicklung des Dienstes die Privatsphäre-Voreinstellungen immer wieder ohne klare Einwilligung der Nutzer verändert hat. Viele Nutzer haben daher schon versehentlich Daten über sich zugänglich gemacht. Das bedeutet, dass sich Nutzer aktiv informieren müssen, welche neuen Funktionen Facebook freischaltet und in welche Richtung sich die Plattform entwickelt, um bei Bedarf ihre Einstellungen zu prüfen und zu korrigieren.

Die für viele Nutzer nicht durchschaubaren Änderungen sorgen zugleich immer wieder dafür, dass sich Mythen über bestimmte Facebook-Funktionen verbreiten. Misstrauisch sollte man immer dann werden, wenn man von den Facebook-Kontakten dazu aufgefordert wird, bestimmte Anleitungen zu befolgen oder Musterformulierungen auf das eigene Profil zu kopieren. Nutzer teilen diese in der Hoffnung, damit einer weiteren Nutzung ihrer Daten zu widersprechen oder sie durch bestimmte Einstellungen einzuschränken. In der Regel sind die Erklärungen wirkungslos und die Einstellungen führen zu anderen als den erhofften Resultaten. Informationen über solche Facebook-Hoaxes sammelt zum Beispiel die Seite mimikama.at.

Welche Daten Facebook sammelt – und was in ihnen steckt

Die Daten, die Facebook über den einzelnen Nutzer sammelt, lassen sich in verschiedene Kategorien einteilen. Das sind erstens diejenigen **Daten, die Nutzer aktiv beitragen**. Bei der Registrierung sind das etwa der Name, der Wohnort, der Geburtstag, das Geschlecht und die E-Mail-Adresse. Diese Angaben sind Pflicht. Nutzer können freiwillig weitere persönliche Informationen eingeben, etwa auf welcher Schule sie waren und wo sie arbeiten. Bei der alltäglichen Nutzung von Facebook kommen viele weitere solcher Daten hinzu, etwa durch „Gefällt mir“-Angaben, Kommentare, Statusmeldungen, das Eingehen von Freundschaften, die Teilnahme an Gruppen und Veranstaltungen, Verlinkungen und Postings, die Kommunikation über die Mail- und Chat-Funktionen und vieles mehr.

Nicht immer sind sich Nutzer bewusst, dass sie Facebook mit ihren Aktivitäten darüber hinaus weitere Informationen übermitteln. So speichert Facebook beispielsweise die Metadaten von hochgeladenen Fotos und Videos. Häufig sind das unter anderem Zeitpunkt und Standort der Aufnahme und das verwendete Gerät (Smartphone, Tablet usw.). Wer über sein Smartphone dauerhaft auf Facebook eingeloggt ist, verrät dem Unternehmen sein alltägliches Bewegungsprofil. Das ergibt eine zweite Kategorie von Daten: solche, die durch – meist automatische bzw. maschinelle – **Beobachtung des Verhaltens** der Nutzer gewonnen werden. Facebook kann hochgeladene Fotos zum Beispiel auch scannen und versucht automatisch zu erkennen, ob etwa lachende Gesichter, ein bestimmtes Essen oder Landschaftsaufnahmen zu sehen sind. Die vor einigen Jahren eingeführte automatische Gesichtserkennung ist nach Angaben des Unternehmens für Nutzer in Europa abgeschaltet.

Das Beispiel der Bilderkennung zeigt, dass man als Nutzer nicht immer weiß, wie viele Informationen Facebook durch die Nutzung erhält. Das gilt umso mehr für den Ansatz, aus den vorhandenen Daten mit statistischen Mitteln neue Informationen zu extrahieren. Solche „Big Data"-Analysen zielen häufig darauf, neue Zusammenhänge (Korrelationen) in den Daten zu entdecken. Die dritte Datenkategorie sind solche, **aus den vorhandenen abgeleitete Daten**. Bereits unsere „Gefällt mir"-Angaben etwa verraten überraschend viel über uns. Britische Forscher konnten über eine Auswertung der „Likes" recht treffsicher abschätzen, ob ein Facebook-Nutzer weiblich oder männlich, homo- oder heterosexuell, christlichen oder muslimischen Glaubens ist. Auch Facebook selbst durchforstet und untersucht die Nutzerdaten, gelegentlich werden einzelne dieser Untersuchungen und Experimente in der Öffentlichkeit diskutiert. So wurde beispielsweise bereits untersucht, ob viele positive oder negative Nachrichten auf Facebook zu einer „emotionalen Ansteckung" führen oder ob sich eine Liebesbeziehung zwischen zwei Nutzern aus der Struktur ihres Gesamtnetzwerks statistisch vorhersagen lässt.

Um neue Informationen zu gewinnen, können zudem verschiedene Datentöpfe kombiniert werden. Nach dem Zukauf weiterer Firmen kann Facebook beispielsweise die Nutzerdaten der Fotoplattform **Instagram** verwenden. Im Fall des 2014 erworbenen Messaging-Dienstes **WhatsApp** hatte Facebook ursprünglich versprochen, die Datenbestände getrennt zu halten. Im Herbst 2016 änderte WhatsApp jedoch seine Richtlinien: Nutzungsdaten und Handynummern sollten nun auch an Facebook übertragen werden. Zwar hatte WhatsApp eine Widerspruchsmöglichkeit vorgesehen, diese wurde aber von vielen Nutzern missverstanden: Sie bezog sich nur auf die Nutzung der Daten zu Werbezwecken, nicht auf die Übertragung der Daten als solche. Nachdem Datenschützer und

Verbraucherverbände in Deutschland dagegen vorgingen, soll der Datentausch seit November 2016 vorerst gestoppt sein, der Streit ist jedoch noch nicht beendet und wird derzeit vor Gericht fortgeführt (Stand Februar 2017).

Zu den Daten, die die Firmen der Facebook-Unternehmensgruppe sammeln, gesellen sich weitere Informationen von **Datenhändlern** und **Marktforschungsunternehmen**. Wie ein Bericht des Magazins c't festhält, nutzt Facebook in Deutschland Daten der Firmen Acxiom und Datalogix, international kooperiert es etwa mit den Unternehmen BlueKai, Epsilon und Quantium. Dadurch können Werbekunden Zielgruppen zusätzlich anhand von Informationen eingrenzen, über die Facebook möglicherweise noch nicht verfügt, etwa den Besitz eines bestimmten Autos. Um verschiedene Datentöpfe richtig zu kombinieren, dienen häufig E-Mail-Adressen, Telefonnummern oder daraus gebildete Prüfsummen als Schlüssel.

Teil 4: Tracking per Like-Button & Co. – und wie Nutzer sich schützen können

Nicht alle Nutzer wissen, dass sie auch dann Daten an Facebook liefern, wenn sie außerhalb von Facebook unterwegs sind: Wenn Webseiten etwa den **„Gefällt mir"-Button** einsetzen, werden im Hintergrund Daten der Besucher zu Facebook geschickt. Dafür muss ein Nutzer nicht unbedingt auf den „Gefällt mir"-Button geklickt haben oder bei Facebook eingeloggt sein. Die Daten werden übertragen, weil die Buttons über einen sogenannten Inlineframe von den Facebook-Servern geladen werden.

Dadurch kann Facebook automatisch erfahren, wer die entsprechenden Seiten aufgerufen hat. Zu den Daten, die übertragen werden, können die Spracheinstellungen des Browsers oder Geräts gehören, der Standort des eigenen Computers, mit welchem Webbrowser man im Netz unterwegs ist, die Bildschirmauflösung und vieles mehr. Außerdem kann die IP-Adresse sichtbar gemacht werden, welche von einigen Datenschützern in diesem Kontext als personenbezogen angesehen wird. Hat man einen Facebook-Account und ist man in diesen eingeloggt, während man surft (dafür muss kein Facebook-Fenster offen sein), erfährt Facebook vom Besuch aller Seiten, die „Gefällt mir"-Buttons oder ähnliche Elemente verwenden.

Verknüpft mit anderen Diensten und Daten kann so ein recht genaues Nutzerprofil erstellt werden. Die Beobachtung des Nutzers im Web kann potenziell sehr umfassend sein. Facebook erklärt dazu, man lösche die erhaltenen Daten innerhalb von 90 Tagen. Auch bei Nutzern, die nicht eingeloggt sind, kann Facebook gleichwohl Daten über eine eigens zugewiesene Kennung sammeln. Es ist möglich, dass auch auf diesem Weg Informationen über das Surfverhalten erfasst werden.

Neben den „Gefällt mir“-Buttons gibt es weitere, von Facebook bereitgestellte **Werkzeuge (Social Plugins)**, die ähnlich funktionieren. Dazu zählen etwa die „Teilen“-Buttons oder Funktionen zur Einbindung von Facebook-Fanseiten oder gepostete Inhalte auf Websites. Nutzer können in den Einstellungen des Browsers festlegen, dass Cookies von Drittanbietern abgewiesen werden, um die Nachverfolgung durch Facebook beim Surfen zu erschweren. Cookies sind jedoch nur ein einzelner technischer Ansatzpunkt beim Tracking. Ihre Sperre kann auch dazu führen, dass andere Funktionen der Webseite nicht mehr funktionieren. In den meisten Browsern lässt sich daneben eine „Do not Track“-Einstellung aktivieren. Diese Funktion dürfte zum Schutz vor Tracking durch Facebook und andere Unternehmen ebenfalls nicht ausreichen, da ihre Befolgung freiwillig ist.

Nutzer können auch **Browser-Erweiterungen** installieren, welche das Tracking unterbinden oder zumindest erschweren. Manche dieser Erweiterungen haben sich jedoch als problematisch erwiesen, da sie sich ebenfalls als ungewollte Datensammler entpuppten. Auch Erweiterungen sollten daher nicht gedankenlos installiert werden. Von der US-Bürgerrechtsorganisation EFF stammt die Erweiterung „Privacy Badger“, welche ohne großen Einstellungsaufwand einsetzbar ist. Sie soll zwar nicht jegliches Tracking unterbinden, sondern durch einen selbstlernenden Ansatz verhindern, dass Nutzer ungefragt über verschiedene Webseiten hinweg verfolgt werden. „Gefällt mir“-Buttons und vergleichbare Funktionen werden von der Erweiterung durch Schaltflächen ersetzt, die erst dann Daten übertragen, wenn man sie tatsächlich verwendet. Der „Privacy Badger“ ist für die Browser Firefox, Chrome und Opera verfügbar. Weitere Schritte und Werkzeuge, mit denen Nutzer sich schützen können, finden sich zum Beispiel bei netzpolitik.org.

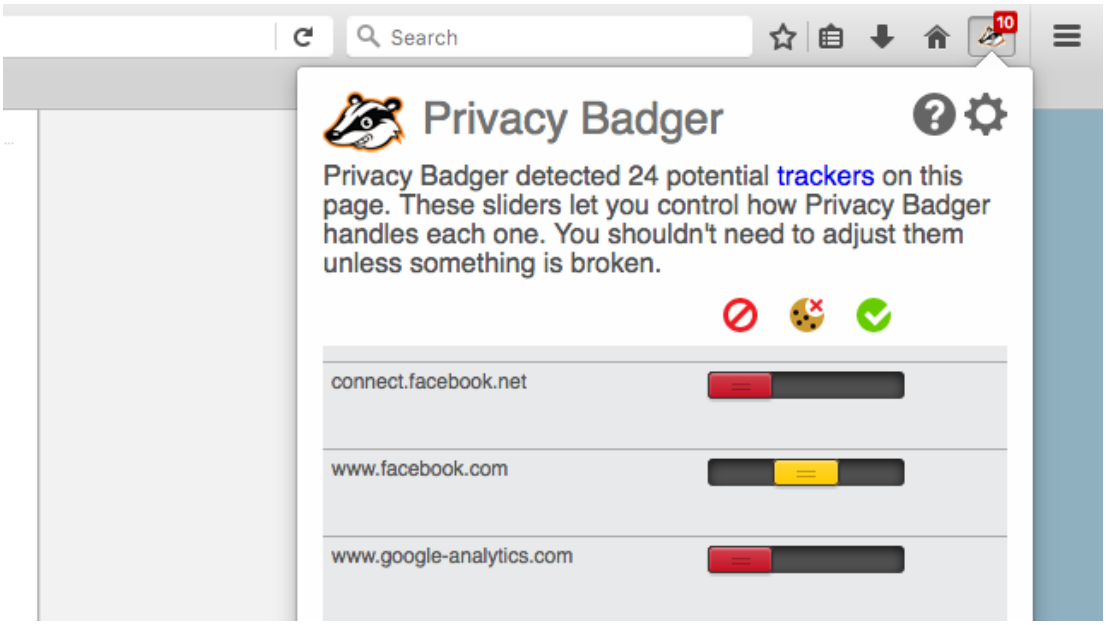

Abbildung 1: Browser-Erweiterungen wie der „Privacy Badger“ können in vielen Fällen verhindern, dass beim Surfen Daten an Facebook fließen (Stand 02/2017)

Auch Webseiten-Betreiber können Datenschutz-freundliche Lösungen einsetzen, wenn sie Buttons zum Empfehlen ihrer Inhalte verwenden. So hat etwa der Heiseverlag die „Shariff"-Buttons entwickelt. Daten der Nutzer werden auch hier erst dann an Facebook übertragen, wenn sie angeklickt wurden. Im Unterschied zu früheren Varianten ist kein zweifaches Klicken mehr erforderlich.

Spiele und Facebook-Login für Websites und Dienste

Auf Facebook können auch Drittanbieter ihre Spiele einbinden. Hierbei werden kleine Programme zum Facebook-Profil hinzugefügt. Wenn man ein Spiel über Facebook verwendet, erhält der Anbieter stets die öffentlich zugänglichen Profilinformationen wie Name, Bild, Altersgruppe und Geschlecht, häufig auch die Freundesliste und die hinterlegte E-Mail-Adresse. In Facebooks App-Center werden die übertragenen Daten unterhalb des „Jetzt spielen"-Buttons angezeigt. Ohne dass man zumindest die Profilinformationen übermittelt, sind die Spiele allerdings nicht nutzbar. Fragt der Anbieter darüber hinaus Daten wie etwa die Freundesliste ab, lässt sich dieser Zugriff über den Link „Von dir angegebene Infos bearbeiten" auch abwählen. Es kann sein, dass Spiele dann nur eingeschränkt verwendbar sind. Bevor Nutzer Dritten Zugriff gewähren, sollten sie stets genau überlegen, ob sie den Anbietern vertrauen. Ein erster Schritt dazu ist zum Beispiel, nach Medienberichten zu suchen.

Auch zahlreiche Websites und Dienste bieten an, das Facebook-Profil zum Erstellen eines Benutzerkontos und zum Einloggen zu verwenden. Ähnlich wie bei Spielen erhält der jeweilige Anbieter Nutzerdaten von Facebook, Facebook wiederum weitere Informationen zum Beispiel über die Interessen seiner Nutzer. Beim ersten Login mit Facebook wird dann angezeigt, auf welche Daten der Anbieter Zugriff erhält.

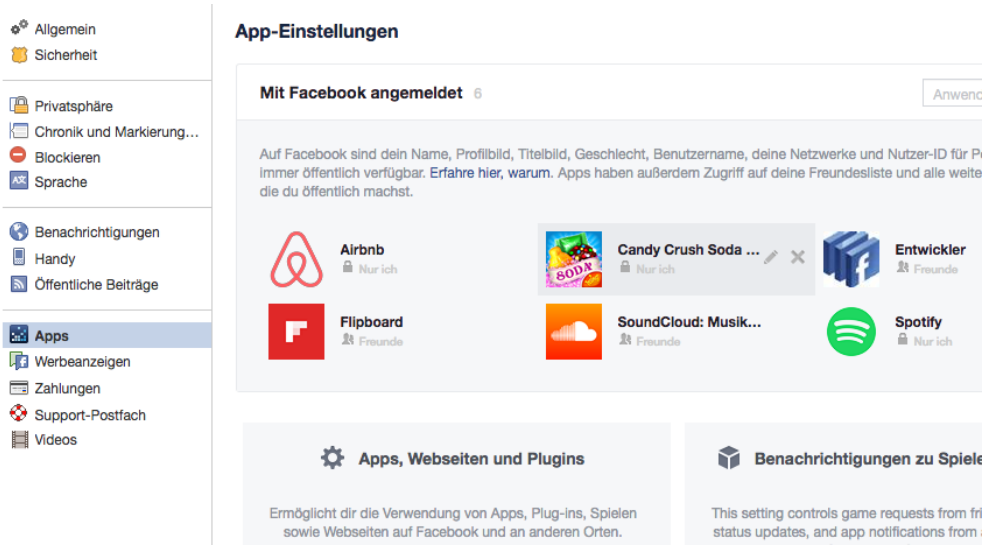

Abbildung 2: Die App-Einstellungen bei Facebook zeigen, wem man Zugriff auf die eigenen Daten gewährt hat (Stand 02/2017)

Bei älteren, vor 2015 üblichen Versionen des Facebook-Logins war zum Teil weniger deutlich, welche Zugriffsrechte erteilt werden, Nutzer hatten dabei auch weniger Eingriffsmöglichkeiten. Wer einen Blick auf die „App-Einstellungen“ wirft (oben rechts unter „Einstellungen“ – „Apps“), findet möglicherweise noch alte Karteileichen unter den Anwendungen. Dort werden alle Spiele, Webseiten und Anwendungen aufgelistet, denen Zugriff gewährt wurde. Es empfiehlt sich, zwischendurch immer mal wieder aufzuräumen und Anwendungen, die man nicht braucht, zu löschen oder die Zugriffsrechte anzupassen.

Wer das Facebook-Login bislang nur aus Bequemlichkeit nutzte, aber den damit verbundenen Datentausch kritisch sieht, wird vielleicht auch mit **Passwort-Managern** glücklich. Solche für alle Geräte und Betriebssysteme erhältlichen Programme helfen beim Erstellen unterschiedlicher Benutzerkonten im Web und speichern die Zugangsdaten auf sichere Weise ab.

Facebook-Nutzer können ebenfalls kontrollieren, auf welche die eigene Person betreffende Informationen Anwendungen zugreifen dürfen, die Freunde verwenden. Denn auch Facebook-Kontakte können diese den Anwendungen, die sie nutzen, zur Verfügung stellen. Will man das nicht, sollte man seine Anwendungseinstellungen bearbeiten und den Zugriff abwählen. Das kann man ebenfalls in den App-Einstellungen unter „Von anderen Personen verwendete Apps“ tun. Für die Facebook-Kontakte selbst bleiben die Informationen je nach persönlicher Einstellung sichtbar.

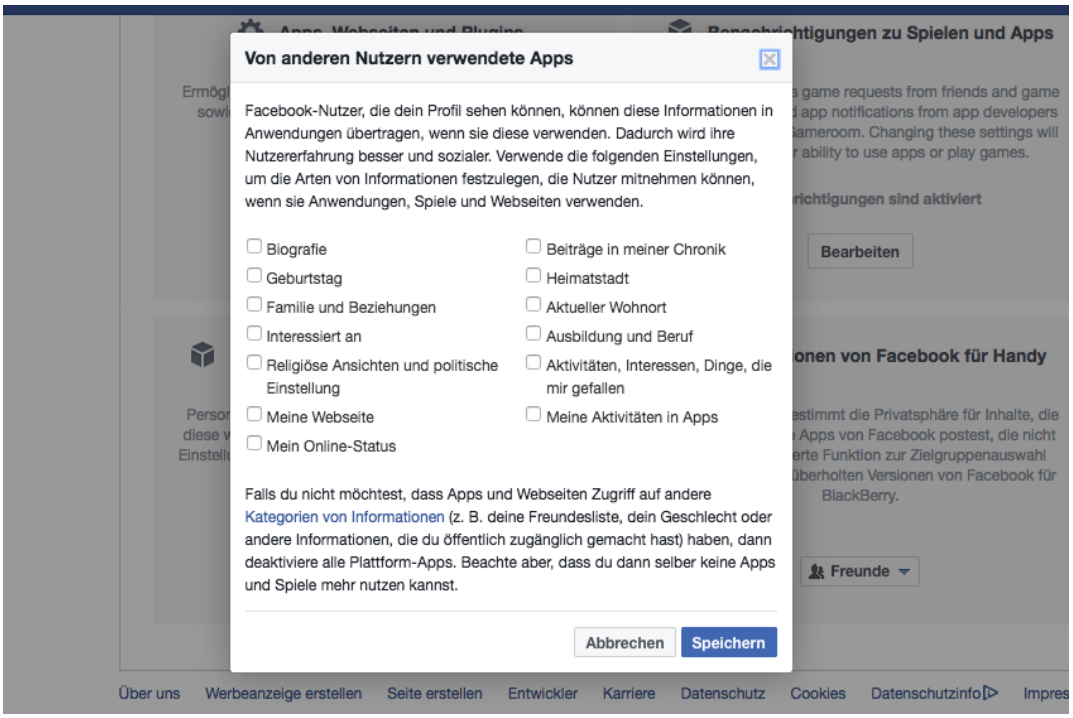

Abbildung 3: Nutzer können einstellen, auf welche Daten die Apps von Facebook-Kontakten zugreifen können (Stand 02/2017)

Damit können Anwendungen von Freunden aber immer noch die öffentlich zugänglichen Informationen auslesen. Will man auch das verhindern, muss man sogenannten Plattform-Anwendungen vollständig deaktivieren (in den App-Einstellungen unter „Apps, Webseiten und Plugins“), kann dann aber selbst keine Spiele, Anwendungen und die Anmeldung über Facebook mehr nutzen.

Wie erfahre ich, welche Daten Facebook über mich gesammelt hat?

Nach deutschem und europäischem Recht hat grundsätzlich jeder Bürger das Recht zu erfahren, welche personenbezogenen Daten über ihn gespeichert wurden. Bei Facebook kommen eine Menge Daten zusammen (siehe oben). Facebook stellt in den allgemeinen Einstellungen einen Link zur Verfügung, mit dem Nutzer sich zahlreiche ihrer bei Facebook gespeicherten Daten herunterladen können (ganz unten unter „Lade eine Kopie deiner Facebook-Daten herunter“). Derzeit enthält der Download unter anderem die veröffentlichten Fotos und Videos sowie zahlreiche Daten im HTML-Format, etwa die Profilinformationen, die Chronik, ausgetauschte Nachrichten, Veranstaltungseinladungen sowie Login-Daten zum Teil mit IP-Adressen. Selbst wenn man kein Problem mit der Datensammelwut von Facebook hat, ist es interessant, einmal zu sehen, wie viel Details seines Lebens man einem Unternehmen zugänglich gemacht hat.

Auch wenn man kein Konto bei Facebook hat, kann man Facebook eine Anfrage schicken, denn es ist gut möglich, dass Facebook dennoch die eigene Person betreffende Daten gesammelt hat, etwa über die Adressbücher von Freunden. Dazu kann man entweder eine E-Mail an „datarequests@fb.com“ schreiben, oder das entsprechende Formular bei Facebook ausfüllen.

Dass man überhaupt Zugang zu seinen bei Facebook gespeicherten Informationen hat, geht unter anderem darauf zurück, dass Aktivisten Druck auf Facebook ausgeübt haben – allen voran das Projekt „Europe versus Facebook“, das beharrlich auf Auskunftsrechte gepocht hat. Man muss aber davon ausgehen, dass auch die herunterladbaren Daten keinen vollständigen Überblick geben. Wer versuchen will, noch umfangreichere Datenbestände über sich zu erhalten, findet auf der Seite von „Europe versus Facebook“ Vorlagen für Auskunftsersuchen, unter anderem auch für Anschluss-Beschwerden bei der irischen Datenschutzbehörde und der EU-Kommission.

Facebook mit Pseudonym nutzen

Um die Nutzung von Facebook mit Pseudonymen gibt es immer wieder Streit. Die Facebook-Nutzungsbedingungen verlangen, dass der Nutzer sich unter seinem echten Namen registriert und nicht mit einem Pseudonym (siehe Facebooks „Erklärung der Rechte

und Pflichten“, Punkt 4). Facebook behält sich vor, Nutzer, die gegen diese Regel verstoßen, auszusperren, was auch immer wieder passiert.

Datenschützer konnten bislang nicht durchsetzen, dass Facebook auch eine pseudonyme Nutzung ermöglicht. Sie argumentieren unter anderen, dass das deutsche Telemediengesetz (Paragraf 13 Absatz 6) Anbieter dazu auffordert, eine anonyme oder pseudonyme Nutzung zu ermöglichen, wenn es technisch machbar und zumutbar ist. Das Oberverwaltungsgericht Schleswig wies entsprechende Beschwerden 2013 jedoch ab, da deutsches Recht bei ihrem Vorgehen nicht anwendbar sei. Zu einem ähnlichen Ergebnis kam 2016 das Oberverwaltungsgericht Hamburg. Der Streit kann jedoch noch weiter gehen.

Ende 2015 kündigte Facebook an, mehr Rücksicht auf Nutzer nehmen zu wollen, die ein besonderes Interesse an pseudonymer Nutzung haben. Bei den Prozeduren zur Namensüberprüfung sollen Nutzer es etwa angeben können, wenn sie diskriminierten oder marginalisierten Gruppen angehören. Nach Facebook-Angaben handelte es sich dabei jedoch nur um einen Test, der zudem auf Nutzer in den USA beschränkt war. Zu wesentlichen Änderungen der Klarnamen-Politik kam es offenbar nicht. Nutzern in Deutschland bleibt also nichts anderes übrig, als sich an die Nutzungsbedingungen zu halten oder zumindest eine Sperrung ihres Benutzerkontos zu riskieren.

Facebook-Account löschen

Man würde meinen, es ist nicht schwierig, das eigene Facebook-Konto zu löschen. Doch so einfach ist es leider nicht. Facebook macht einem den Austritt nicht leicht. Auf den ersten Blick bietet das Netzwerk seinen Nutzern nur die Möglichkeit, den Account zu deaktivieren. Dabei bleiben aber alle Daten und Einstellungen erhalten; sie sind nur nicht mehr zu sehen. Entscheidet man sich später, Facebook weiter zu nutzen, kann man wieder da anfangen, wo man aufgehört hat. Die Option, das Konto tatsächlich zu löschen, findet sich etwas versteckt im Hilfebereich unter „Mein Konto löschen“. In dem klicksafe-Leitfaden „Sicher unterwegs in Facebook“ (PDF) wird unter Punkt 9 Schritt für Schritt erläutert, wie man sein Konto löschen kann.

Hat man die Löschung seines Kontos beantragt, kann es eine Weile dauern, bis es wirklich weg ist. Facebook verzögert die endgültige Löschung um circa 14 Tage, falls man es sich doch anders überlegt. Loggt man sich innerhalb dieser Zeit wieder bei Facebook ein, wird die Löschung gestoppt. Danach kann es noch einmal bis zu 90 Tage dauern, bis wirklich alle zugehörigen Daten gelöscht sind. Die Kommentare, die man zum Beispiel auf Facebook hinterlassen hat, erscheinen dann unter dem Namen „anonymer Facebook-Nutzer“. Will man sicher gehen, dass auch sämtliche solcher Spuren verschwinden,

muss man das vor der eigentlichen Löschung des Profils per Hand machen. Einen Überblick bietet das eigene **Aktivitätenprotokoll** (erreichbar oben rechts auf Facebook).

Weiterführende Informationen

- Facebook: Nutzungsbedingungen und Richtlinien
- klicksafe.de: Informationen und Leitfäden zum Schutz der Privatsphäre in Facebook
- klicksafe-Publikationen u. a. zu den Themen Datenschutz und soziale Netzwerke
- iRights.info: Beiträge zum Thema Facebook und Social Networks