Hungriges Datenmonster

Was Facebook mit Ihren Daten macht

Der Begriff „Datenkrake“ wird hierzulande meist synonym zu Google verwendet. Facebook ist allerdings in vielerlei Hinsicht der größere Datensammler. Ein Blick in die Datenbanken des sozialen Netzwerks.

Von Jo Bager

Facebooks Hunger auf Daten lässt sich nicht stillen – daran wurden die Nutzer zuletzt Ende August erinnert. Hatte Facebook 2014 beim Kauf von WhatsApp noch hoch und heilig versprochen, die Nutzerdaten des beliebten Messengers nicht anzurühren, so streckt die Mutterfirma nun doch die Finger nach Telefonnummern und Aktivitätslogs der Anwender aus. Hierzulande wird sie dabei vom hamburgischen Datenschützer ausgebremst, der ihr die Datenübertragung bislang untersagt hat. Doch dagegen geht Facebook vor Gericht.

Die Ankündigung der Datenübertragung hat für reichlich Verunsicherung unter den 35 Millionen deutschen WhatsApp-Nutzern gesorgt. Viele fragen sich, ob man die App überhaupt noch verwenden soll. Doch das Aufheben um WhatsApp vernebelt den Blick auf das große Ganze: Auf die Tatsache nämlich, dass Facebook der ganz große Datensammler ist und an vielen Stellen im Netz Informationen absaugt.

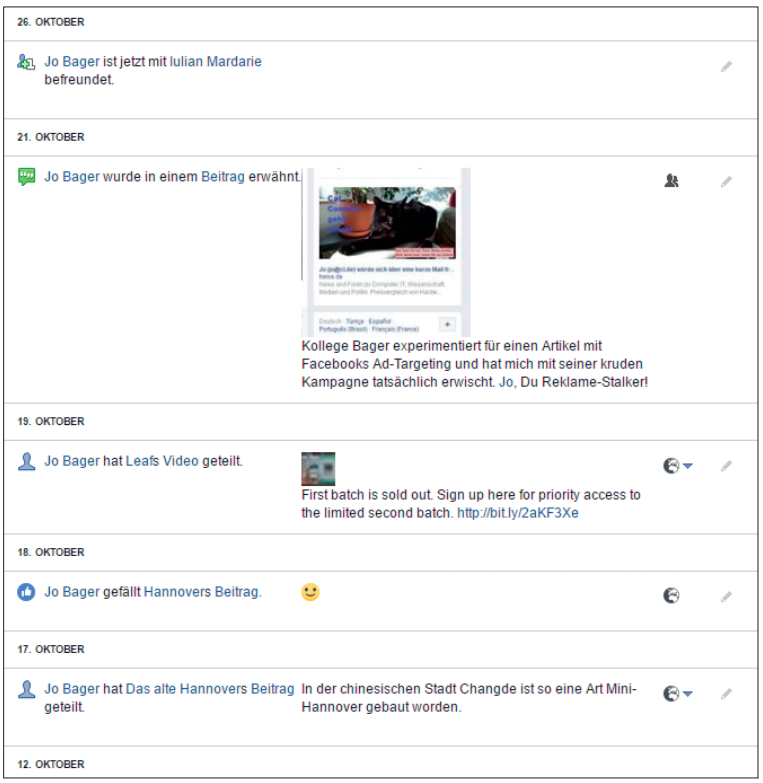
Dieser und die folgenden Artikel nehmen Facebooks Datensammelei daher genau unter die Lupe: Warum sich Facebook eigentlich so viele Daten einverleibt, was damit passiert und was das für den Einzelnen bedeutet, erklärt dieser Beitrag. Der Artikel auf Seite 76 dröselt auf, aus welchen Quellen die Daten stammen und wie die Sammelei technisch vonstatten geht.

Ab Seite 80 zeigen wir, wie Sie herausfinden, was Facebook über Sie weiß oder zu wissen glaubt und wie Sie unerwünschte oder falsche Informationen löschen oder berichtigen. Der Beitrag ab Seite 84 schließlich beleuchtet die juristische Seite der Facebook’schen Datenerhebung und die Bemühungen des Österreichers Max Schrems um mehr Datenschutz bei Facebook.

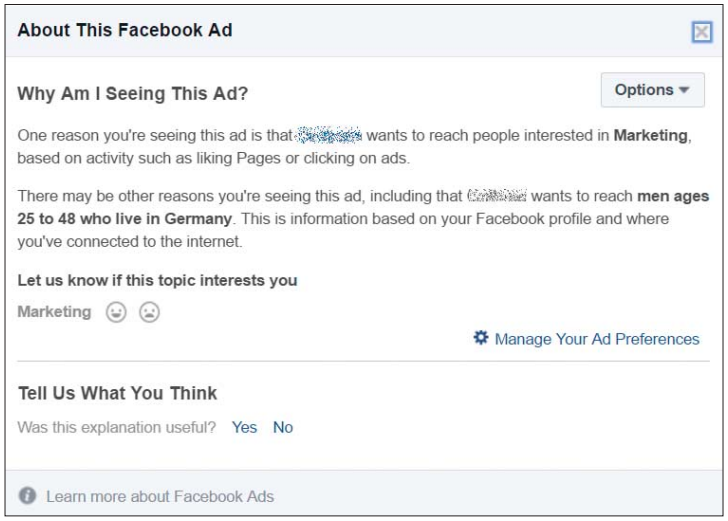
Im Maschinenraum

Wann immer ein Nutzer einen Link oder Kommentar postet, jemanden auf einem Foto markiert oder seine Lieblingsband mit einem „Like“ versieht, gibt er Facebook Informationen über sich preis. Werfen Sie einmal einen Blick in Ihr Aktivitätenprotokoll (siehe c’t-Link). Dort hält Facebook minutiös fest, was Sie alles auf der Plattform gemacht haben.

Facebook kennt aber in der Regel auch wesentliche Teile Ihres sozialen Netzwerks und weiß, wann Sie bestimmte Websites aufrufen. Bei etlichen Apps kriegt Facebook mit, wann Sie sie einsetzen – und zwar bei weitem nicht nur bei



Facebook merkt sich genau, was man wann auf der Plattform macht.



Bei jeder Werbeanzeige auf der eigenen Plattform legt Facebook Rechenschaft darüber ab, aufgrund welcher Zielgruppendaten sie ausgewählt wurde.

denen der Töchter WhatsApp und Instagram. Facebook zapft sogar Quellen an, die Ihr analoges Leben jenseits des Internet kennen (siehe S. 76).

All diese Informationen bündelt Facebook, um Werbung zu verkaufen, denn das ist das Geschäftsmodell des Unternehmens – und zwar ein sehr einträgliches. Werbung trug im zweiten Quartal 2016 6,2 Milliarden zu den Gesamtumsätzen von 6,4 Milliarden US-Dollar bei, bei insgesamt 2,1 Milliarden Dollar Gewinn. Facebook punktet damit, seine Nutzer sehr zielgenau mit sogenanntem Targeting ansprechen zu können, also mit speziell auf die Interessen der Benutzer zugeschnittenen Anzeigen.

Und welches Bild hat Facebook über Sie? Wer nicht wie Max Schrems unter einigen Mühen das komplette Dossier per Auskunftsersuchen anfordern will (siehe S. 84), kann in den „Einstellungen für Werbeanzeigen“ zumindest einen Einblick erhalten. Aufrufen lassen sich diese über die persönlichen Einstellungen oder das zu jeder Facebook-Werbung gehörende Menü.

Dann erscheint eine Liste mit Themen, Unternehmen, Produkten und Dienstleistungen, von denen Facebook glaubt, dass sie Sie interessieren könnten. Wenn Sie mit Ihrem Mauszeiger über die angezeigten Themen fahren, bekommen Sie sogar angezeigt, warum Facebook das relevant für Sie hält. Falls momentan passende Anzeigen auf Facebooks Werbeplattform geschaltet werden, erscheinen diese ebenfalls.

Im Falle des Autors dieses Artikels kommt dabei eine Mischung aus gut treffenden, aber auch einigen merkwürdigen Einschätzungen zusammen: „Info über Facebook for Android – Du hast diese Einstellung, weil du die App Facebook for Android installiert hast“ – stimmt. „(13–18 Jahre) Eltern mit Teenagern“ – passt. Aber wie kommt Facebook darauf, dass ich mich für die Bibel interessieren könnte, oder für „Lehnswesen“? „Du hast diese Einstellung, weil du eine Werbeanzeige im Zusammenhang mit Lehnswesen angeklickt hast“ – muss länger her sein, ich kann mich nicht daran erinnern.

Facebook gewährt seinen Nutzern diese Einblicke natürlich nicht selbstlos, eher im Gegenteil. Vielmehr soll der Anwender hier unzutreffende Interessen löschen, also: Sein Profil für Facebook zusätzlich schärfen.

Rasterfahndung

Beim Targeting geht es nicht darum, den einzelnen Kunden zu adressieren, also zum Beispiel mich, Jo Bager, persönlich. Auch handelt Facebook nicht mit den Daten; diesen Informationsschatz gibt das Unternehmen nicht aus den Händen. Vielmehr schalten Werbetreibende Anzeigen, die bestimmte Zielgruppen erreichen sollen.

Aus 1300 Kategorien kann jeder Werbetreibende sein Zielpublikum herauspicken. Nach der Auswahl der Basisdaten – Ort, Alter, Geschlecht, Sprache – gehts ans Eingemachte: Schulabschluss, Arbeitsbranche, Monatseinkommen und Beziehungsstatus lassen sich einfach an- und abwählen. Soll die Zielgruppe eine Fernbeziehung, einen neuen Job oder bald Geburtstag haben? Interessiert sie sich für Festplatten, Freizeitparks, Golf, Landwirtschaft, Mangas, Militär, Motorroller, Reptilien, Schlagzeug, Schokolade, Talkshows, Tattoos, Yoga? Fährt sie BMW, benutzt sie Linux, besitzt sie Aktien, zieht sie häufig um? 12 Millionen Facebooker leben in einer komplizierten Beziehung, 33 Millionen interessieren sich für Nagelpflege, 155 Millionen hören gerne Funk.

Einen guten Eindruck von Facebooks Möglichkeiten erhält man mit einem kleinen Perspektivwechsel, nämlich indem man eine eigene Werbung platziert. Das haben wir ausprobiert und eine Kampagne gestartet, die auf c’t-Kollegen ausgerichtet war: Über 18, im Umkreis von Hannover wohnend, an Computern interessiert und bei Heise angestellt. Die Werbung lief zwei Tage; von einem halben Dutzend Kollegen kam die Rückmeldung, dass sie sie gesehen haben.

Blasen-Forschung

Facebook benutzt die Kenntnisse über seine Nutzer auch, um die in deren Timelines angezeigten Informationen einzuschränken. Kein Mitglied des sozialen Netzwerks bekommt alle abonnierten Inhalte zu Gesicht; das wären in aller Regel zu viele. Daher filtert Facebook vor und versucht nur diejenigen Posts anzuzeigen, die die Benutzer besonders interessieren. Das erzeugt den sogenannten Filterblasen-Effekt: Nutzer bekommen eher solche Posts zu sehen, die ihre Meinungen bestätigen, andere Ansichten werden ausgeblendet.

Facebook ist längst nicht mehr nur ein Kommunikationswerkzeug, sondern für viele Menschen auch eine wichtige Nachrichtenquelle. Die Plattform wird mehr und mehr zu einem Massenmedium, die mit ihren Filtern bestimmt, was seine 1,7 Milliarden Nutzer zu sehen bekommen – ein riesiges Machtinstrument. Das bestätigen auch Facebooks eigene Forscher, die gerne einmal die Plattform als sozialwissenschaftliches Experimentierfeld nutzen.

So haben sie im Jahr 2012 mit den Stimmungen der Mitglieder herumgespielt. Zwei Gruppen wurden jeweils eher optimistische oder pessimistische Postings

ihrer Freunde gezeigt. Das hatte den Effekt, dass die Gruppen in der Folge auch eher positive oder negative Posts veröffentlicht haben. Mit einem Experiment während der US-Wahlen 2010 und 2012 konnten Facebooks Forscher zudem den Beweis erbracht haben, dass das Netzwerk durch kleine Modifikationen in den Timelines sogar eine Wahl entscheiden kann, die auf der Kippe steht (siehe c't-Link).

Nicht jede Information, die sich aus Facebooks Datenschatz herauslesen lässt, liegt dort mit der Zustimmung der Betroffenen. Das zeigen immer wieder Beobachtungen im Zusammenhang mit dem Freundefinder. Dieser empfiehlt Mitgliedern Menschen, zu denen sie tatsächlich eine irgendwie geartete Verbindung haben – von der sie sich aber nicht vorstellen konnten, dass Facebook sie kennen kann. Der amerikanische Webdienst Fusion berichtete im Juni von einer Psychaterin, die so eine Erfahrung gemacht hat. Obwohl sie, wie sie beteuert, ihr Adressbuch nicht hochgeladen hatte, begann Facebook plötzlich, ihr ihre Patienten als Freunde vorzuschlagen. Schlimmer noch: Mehreren ihrer Patienten sind andere Patienten als Freunde vorgeschlagen worden – ein unter Umständen schon gefährliches Outing.

Fatale Verknüpfungen

Bei den Freundefinder-Empfehlungen bleiben die Informationen zumindest innerhalb des Netzwerks, Facebook gibt sie ja nur an die betroffenen Mitglieder weiter. Aber externe Parteien zeigen natürlich ein großes Interesse an den bei Facebook lagernden Daten. Zum Beispiel für das Scoring: Das Hamburger Unternehmen Kreditech zieht bei seinen Bewertungen für die Kreditvergabe auch Social-Media-Daten mit heran: Mit wem ist der potenzielle Kreditnehmer befreundet? In welcher Lebenslage befindet er sich? Und wie kommuniziert er? Wohl dem, der den richtigen Freundeskreis hat und diejenigen Dinge liked, die Kreditechs Algorithmen als positiv ansehen. Insgesamt will das Unternehmen 20.000 Datenpunkte innerhalb von Sekunden auswerten. Dazu gehören nach Präsentationen von Kreditech auch Informationen, die aus Facebook stammen. Woher es diese Daten bezieht und was es mit ihnen macht, verrät das Unternehmen nicht.

Das britische Unternehmen Score Assured will Vermietern auf ähnliche Weise generierte Auswertungen aus den Social-Media-Aktivitäten von potenziellen Mietern verschaffen. Bereits fast die Hälfte der Personalverantwortlichen recherchiert nach einer Statistik des Portals Statista in den Online-Profilen von Bewerbern, um mehr über sie zu erfahren. Fünfzehn Prozent hätten aufgrund von dort gefundenen Informationen sogar schon Bewerber nicht eingeladen oder nicht eingestellt.

Behörden interessieren sich ebenfalls für Facebooks Daten – das ist spätestens seit den Veröffentlichungen von Edward Snowden bekannt. Das Unternehmen ist zur Kooperation mit US-Geheimdiensten gezwungen, darf aber nicht darüber berichten.

Aus Snowdens Veröffentlichungen wurde bekannt, dass Facebook zudem in der Vergangenheit im Auftrag der US-Regierung regierungskritische Veranstaltungsinfos und Direktnachrichten zwischen teilnehmenden Nutzern manipuliert hat, um Demonstrationen zu verhindern. Egal ob Scoring oder staatlicher Eingriff: Oft hat man nicht einmal die Chance, von den Zugriffen und Manipulationen zu erfahren.

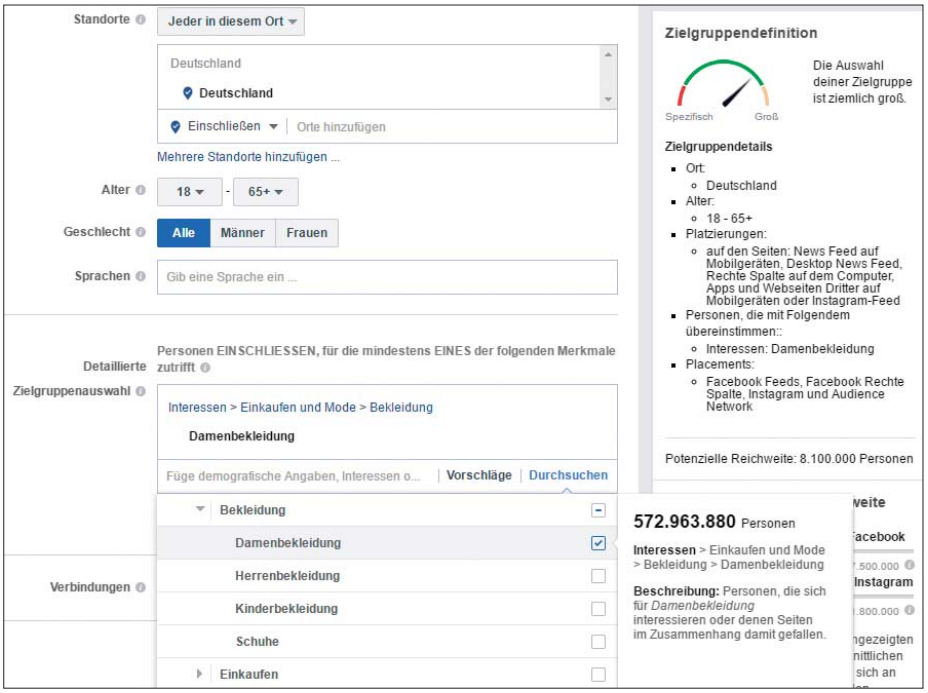
Daten machen Leute

Man mag Facebooks Datenhunger damit abtun, dass der Deal nun mal auf diese Weise funktioniert: Das Unternehmen hält eine Plattform bereit, auf der man sich mit Freunden und Kollegen trifft und austauscht. Facebook erhält dafür die Daten und schneidet damit Werbung zielgenau auf seine Nutzer zu.

In einer durchdigitalisierten Welt sind die Daten über einen Menschen allerdings mehr als nur ein paar Informationsfetzen oder ein Abbild. Die Daten über Sie machen vielmehr ein gutes Stück weit aus, wer Sie *sind*: Die Daten beeinflussen, mit wem Sie in Kontakt kommen, wie andere Sie sehen und welche Inhalte Sie zu sehen bekommen; mitunter wirken sie sich auf wichtige Lebensentscheidungen aus, etwa bei der Wohnungs- und Jobsuche.

Facebook weiß sehr viel über seine Mitglieder, und auch über Menschen, die gar keinen Account bei der Plattform haben. Daher sollte sich jeder die Zeit nehmen und genau kontrollieren, welche Daten das Netzwerk über ihn speichert und sie gegebenenfalls korrigieren. Die folgenden Artikel helfen dabei. *(jo@ct.de)* c't

Weiterführende Informationen:
ct.de/ybn2



Unternehmen können Werbung auf Facebook genau für spezifische Zielgruppen zuschneiden.

Sammelleidenschaft

Wie und wo Facebook seine Daten zusammenträgt

Klar ist: Facebook sammelt sehr viele Daten über seine knapp zwei Milliarden Mitglieder, und auch der Rest der Menschheit gerät in den Gravitationsstrudel dieses schwarzen Datenlochs. Aber wie genau kommt Facebook an die Informationen?

Von Herbert Braun

Facebook erfährt innerhalb der eigenen Plattformen auf fünf Weisen Neues: Indem es erstens auswertet, was Nutzer aktiv über sich angeben, was sie zweitens indirekt durch ihre Aktionen wie liken oder posten hinterlassen und was drittens Nutzer über andere verraten, etwa durch Taggen von Fotos. Außerhalb seiner Plattformen sammelt Facebook viertens fleißig jene Spuren, die Nutzer beim Surfen oder beim Einsatz von Apps hinterlassen – und zwar mithilfe von Codeschnipseln in Websites und Apps. Als Fünftes kommen noch aufgekaufte externe Datenbanken hinzu.

Die meisten aktiv eingegebenen Inhalte finden sich auf der „Info“-Seite jedes Profils: Ausbildung, Beruf, Lebensstationen, Adresse, Kontaktdaten, Familienmitglieder, Profilfoto. Hier hat der Nutzer die Kontrolle, was er preisgibt. Der Übergang zur zweiten Kategorie, den impliziten Daten, ist fließend. Ein hochgeladenes Foto enthält nicht nur Pixel, sondern in der Regel auch Metadaten über Kamera sowie Zeit und Ort der Aufnahme.

Durch Bilderkennungsalgorithmen lassen sich auch die Inhalte maschinell auswerten. Dass Facebook routinemäßig solche Techniken einsetzt, zeigt sich schon an der Bitte, den meist korrekt ermittelten Gesichtern auf dem Foto Namen zuzuweisen. Facebook versucht bereits seit Längerem, die Gesichter auf Fotos automatisch zu erkennen und zu kennzeichnen („photos that look like you“). Dies passiert bislang nach unserer Kenntnis nur in den USA.

Bei Status-Updates, geposteten Links und den standardmäßig nicht Ende-zu-Ende-verschlüsselten Chats im Messenger analysiert Facebook vermutlich die

Schlagworte – und sei es auch, indem es sie für allgemeine Auswertungen à la Google Trends aggregiert. Der mobile Client fügt jedem Posting Standortinformationen hinzu, solange man das nicht abstellt.

Unabhängig von Beiträgen jeder Art kann Facebook die Aktivitäten seiner Nutzer umfassend nachverfolgen, zum Beispiel das reine Leseverhalten. Beim Herumsurfen auf der Seite lassen bereits die Standard-HTTP-Header erkennen, wann und wie lange ein Benutzer Zeit für den Newsfeed hat, welche Beiträge er öffnet und ob er das vom stationären Rechner oder vom Mobilgerät aus tut.

Eine grobe Ortung lässt die IP-Adresse zu. Auf dem Mobilgerät haben Facebook- und Messenger-App in der Regel Zugriff auf die Ortungsfunktion. Damit könnten die Apps zu jeder Zeit den Standort des Nutzers nach Hause funken, auch wenn die App nur im Hintergrund läuft. Den Standort soll zumindest der Messenger nach Angaben von Facebook allerdings nicht verraten. Andererseits erklärt Facebook in seiner Data Policy explizit, Standortdaten zusammen mit Geräte-, Browser- und Verbindungsinformationen aufzuzeichnen.

Likes, Shares und Kommentare verbinden einen Nutzer sowohl mit anderen Profilen oder Seiten als auch mit bestimmten Themen – äußerst wichtig für Facebooks Werbekunden. Wenn ich ständig die Katzenfotos einer Freundin like, kann Facebook daraus sowohl mein Interesse an Katzen wie an der Posterin erschließen. Indizien dafür liefert aber bereits das Ausklappen abgekürzter oder zusätzlicher Beiträge, das Öffnen von Links beziehungsweise Fotos in der Einzelansicht oder das Einblenden verborgener Kommentare.

Im Zentrum jedes sozialen Netzwerks stehen die Verbindungen zu anderen Mitgliedern. Kein Wunder also, dass sich Facebook alle Mühe gibt, bestehende Kontakte auf seiner Plattform abzubilden. So erklären sich die teilweise penetranten Versuche, Nutzer zum Upload ihres Adressbuchs zu nötigen. Auf diese Weise gelangen auch Daten über Nichtmitglieder zu Facebook. Melden diese sich irgendwann einmal an, finden sie sich sofort in ihr soziales Umfeld eingebettet.

Weniger bekannt ist, dass Facebook als Internet-Provider agiert.

Daten-Zuträger

Nicht alle Informationen, die Facebook über eine Person besitzt, stammen von dieser selbst. Ein bekanntes Beispiel dafür ist das Taggen von Fotos – auf diese Weise kann das Netzwerk auch manche Personen erkennen und mit anderen in Verbindung bringen, die kein eigenes Facebook-Profil haben.

Mitunter scheint es zu genügen, dass sich zwei Mitglieder am selben Ort ungefähr zur selben Zeit aufhalten, damit sie einander als Freunde vorgeschlagen werden. Dass sich Facebook für das Freunde-Finden mit der räumlichen Nähe auseinandergesetzt hat, geht zumindest aus einem Patent des Unternehmens aus dem Jahr 2012 hervor. Und es würde auch die mysteriösen Freunde-Empfehlungen aus dem Artikel auf Seite 72 erklären.

Such- und Freundschaftsanfragen können als Indiz gelten, dass zwischen zwei Personen Kontakt besteht. Das gleiche gilt für Erwähnungen von Nutzern, Beiträge in der Timeline eines Profils oder wiederholtem Austausch, etwa in den Kommentaren zu Beiträgen oder im Messenger. Viele Lebensereignisse bieten die Möglichkeit, eine Person einzubeziehen, etwa „in Beziehung mit“; der oder die Betreffende kann dieses Ereignis dann der eigenen Timeline hinzufügen. Ein gegenteiliges Signal sendet das Stummschalten von Freunden, das Entfreunden oder Blockieren. Einladungen zu Veranstaltungen, geschlossenen Gruppen, Apps oder Spielen bringen ein Profil mit dem jeweiligen Thema in Verbindung.

Auch von Firmen erhobene Daten können bei Facebook landen. Angenommen, ein Unternehmen möchte bereits bestehenden Kunden auf Facebook Werbung für ein neues Produkt zeigen. Dazu speist es seine Kundendatenbank oder die Teilnehmer eines Preisausschreibens mit Namen, Mail-Adressen und Telefonnummern in eine sogenannte „Custom Audience“-Liste ein. Diese gleicht Facebook mit bestehenden Profilen ab, um ihnen gezielt die Werbung zu zeigen. Nach Facebooks Angaben läuft dieser Abgleich jedoch nur über Hash-Werte ab, die anschließend gelöscht werden.

Wachsendes Imperium

Facebook sammelt nicht nur in den eigenen Mauern Daten, auch die Tochterunternehmen steuern viele Informationen bei. WhatsApp zum Beispiel überträgt die Telefonnummern und die Nutzungszeiten seiner Anwender. Und das 2012 aufgekaufte Instagram – mit zirka 500 Millionen aktiven Benutzern ein weiterer Web-Gigant – liefert ebenfalls fleißig Daten an den Mutterkonzern. Instagram räumt sich mit seinen Datenschutzbedingungen das Recht ein, „Cookies, Protokolldateien, Gerätekennungen, Or-

Facebook erhebt nicht nur selbst Daten, sondern ermöglicht es auch Dritttunternehmen, Kontaktlisten hochzuladen.

tungsdaten und Nutzungsdaten“ an Facebook zu übertragen.

Weniger bekannt ist, dass Facebook in zunehmendem Umfang auch als Internet-Zugangsprovider agiert. In derzeit 53 Entwicklungsländern in Afrika, Ostasien und Lateinamerika bietet es im Rahmen von internet.org sein „Free Basics“-Paket fürs mobile Surfen an. Aktuell nutzen 40 Millionen Menschen diesen kostenlosen Internetzugang.

Ein Auszug aus den Datenschutzbedingungen von Free Basics: „Wir sammeln beschränkte Geräte-, Browser- und Nutzungsinformationen, wenn du Free Basics verwendest. Insbesondere sammeln wir die Art des von dir verwendeten Geräts bzw. Browsers und Betriebssystems, deine App-Version, App-ID und Geräte-ID, die Zeit und das Datum deiner Verbindung, deinen Mobilfunkanbieter, deine IP-Adresse, deine Telefonnummer, deine Batterie- und Signalstärke, dein Land, deine Spracheinstellung und die Dienste Dritter, nach denen du in Free Basics suchst bzw. die du dort nutzt.“ Ähnlich dicht an der Quelle sitzt die Facebook-Tochter Onavo, die für Android und iOS kostenloses VPN anbietet und deren Datenschutzbedingungen ganz ähnliche Klauseln enthalten.

Die anderen Facebook-Akquisitionen spielen in Sachen Datenaufkommen nicht in der gleichen Liga, sollten aber dennoch nicht übersehen werden. Bekannt ist vor allem das VR-Unternehmen Oculus. Die Fitness-App Moves begleitet die Nutzer beim Joggen und Radeln. Dazu kommen noch diverse Apps, die Facebook unter eigenem oder unter Instagrams Namen herausgibt. Bei den meisten ist der Bezug zum Netzwerk offensichtlich, aber etwa bei der beliebten Spaß-Video-App MSQRD („Masquerade“) oder dem Animationsgenerator Boomerang nicht unbedingt.

Überall mitgeloggt

Bei der Datensammlung Facebooks außerhalb der eigenen Plattform und der Töchter wird jeder als Erstes an den allgegenwärtigen Like-Button denken. Daneben gibt es aber noch diverse andere solcher sogenannter Social Plug-ins, die Website-Betreiber gerne einbinden. Mit den Share- und Quote-Plug-ins etwa teilt man Links oder Textauszüge; über das Send-Plug-in geht das auch via Messenger. Mit „Save“ speichert man Inhalte in einem privaten Bereich auf Facebook, mit dem Follow-Plug-in abonniert man die Updates eines bestimmten Accounts.

Mit weiteren Social Plug-ins lassen sich Facebook-Inhalte in externe Seiten einbinden – Videos, einzelne Beiträge, Kommentare oder eine Übersicht über eine Facebook-Seite (Page-Plug-in). Das Comments-Plug-in schließlich nutzt Facebooks Infrastruktur, um Leser für Kommentare zu authentifizieren und diese mit deren Accounts zu verbinden.

Bei allen seinen Social Plug-ins schlägt Facebook vor, diese über ein JavaScript einzubinden, das direkt vom Facebook-Server kommt. Auf diese Weise erfahren die Server in Menlo Park von jedem Aufruf der betreffenden Seite. Die meisten Menschen dürften nicht wissen, dass Facebook so ihre Klicks auf vielen Sites verfolgen kann. Auf größeren deutschen Websites trifft man den Like-Button in seiner ursprünglichen Form nicht mehr überall an – möglicherweise hat das „Shariff“-Projekt der c’t hier etwas bewegt (siehe Seite 80). Dieses sorgt dafür, dass die Facebook-Server erst kontaktiert werden, wenn der Nutzer den Button anklickt.

Das heißt aber nicht, dass alles gut wäre. Unter Webmastern mangelt es bei der Einbindung von Fremdservern an Datenschutzsensibilität – es gibt populäre Websites, die Inhalte von mehr als einhundert Domains einbinden. Da überrascht es nicht, dass gerade facebook.com beim Aufruf der meisten größeren Websites angefunkt wird. Weniger bekannt ist, dass auch viele Apps Inhalte von Facebook einbetten, zum Beispiel Spotify, Shazam, Tinder und Blendle.

Facebook Login ist eine praktische Authentifizierungslösung. Facebook-Mitglieder können damit ihren Account nutzen, um sich auf Drittanbieter-Webdiensten oder in Apps einzuloggen. Sie müssen sich also ein Passwort weniger merken. Mehrwert für Facebook: Das Unternehmen erfährt, welche Dienste und Apps seine Mitglieder nutzen, und wann. Mit dem „Account Kit“ eröffnet Facebook auch Menschen, die keinen Facebook-Account haben, diese Möglichkeit. Zur Registrierung benötigt Facebook deren Mobilfunknummer oder E-Mail-Adresse.

Kekspackung

Weitere Informationen kommen durch Facebooks Werbebanner außerhalb des Netzwerks zusammen. Das „Audience Network“ ist für Mobilgeräte gedacht und kommt in Apps wie in Mobil-Websites zum Einsatz. Zur Erfolgskontrolle und Konversionssteigerung hält der Konzern das Zählpixel „Facebook Pixel“ und seine Analytics-Lösung für Apps bereit. Die

Bild: Facebook

Aus allen Daten das Maximum herausholen: Für Facebook sind Bilder längst mehr als Pixelhaufen. Es kann sie analysieren und per Text beschreiben.

technische Basis für die zielgruppengerechte Werbung über alle Geräte hinweg kaufte Facebook 2013 von Microsoft: Atlas Solutions, einen Adserver mit Reichweitenmessung und Facebooks Gegenstück zu Googles DoubleClick.

Seit Mai dieses Jahres sammelt Facebook explizit auch von Nichtmitgliedern Daten, um maßgeschneiderte Banner ausliefern zu können. Eine gerichtliche Auseinandersetzung mit der belgischen Datenschutzbehörde über diese Praxis gewannen die Kalifornier im Juni. Bei diesem Prozess ging es um Cookies, mit denen Facebook auch außerhalb der eigenen Plattform Werbung ausliefern und Nutzerdaten analysieren kann.

Auch in Deutschland sammelt Facebook so Daten ein, sowohl für Mitglieder der Plattform als auch für Nichtmitglieder. Nichtmitglieder erhalten allerdings viel weniger Cookies als Mitglieder: Bei einigen Stichproben mit Seiten, die Facebook-Widgets nutzen, schickte uns Facebook im ausgeloggten Zustand fast nirgends ein Cookie; nur bei bild.de fingen wir uns eines namens „fr“ ein – zusammen mit gut 200 Cookies von über 80 anderen Domains.

Wer eingeloggt ist, wird in seinem Browser ein Dutzend kleine facebook.com-Cookies mit überwiegend langer Laufzeit finden, deren genaue Funktionsweise unserem Wissen nach nicht öffentlich dokumentiert ist. Am häufigsten aktualisiert werden „presence“ und „fr“, die mit etwa 160 beziehungsweise 80 Zeichen auch die umfangreichsten sind. „c_user“ enthält die Benutzer-ID und soll zusammen mit „datr“ und „xs“ eingeloggte Benutzer authentifizieren.

Nach eigenen Angaben verwendet Facebook die Cookies außerdem, um Identitätsdiebe oder Spammer zu erkennen, um (etwa in den Plug-ins) ortsbezogene Inhalte auszuliefern oder Einstellungen zu berücksichtigen sowie für die Verbesserung der Performance. Zusätzliche Einstellungen speichert Facebook im localStorage unter www.facebook.com, offenbar aber nicht zum Zweck der Identifizierung.

Datenkauf und -verschmelzung

Um Werbung noch gezielter auf seine Mitglieder zuzuschneiden, als das mit den eigenen Profilen ohnehin schon möglich ist, arbeitet Facebook mit externen Datenhändlern zusammen. Deren Informationen stammen teils von Werbenetzwerken, teils aber auch aus Quellen außerhalb des Internet – Personendaten, Einkaufsgewohnheiten, Autoregistrierungen, Beruf, Familie, Finanzdaten, Urlaubswünsche und vieles mehr.

Gefällt mir: Nur ein kleiner Knopf, aber er ermöglicht es Facebook, mitzuschneiden, wer die Seite besucht.

Facebook bezieht in Deutschland Daten von Acxiom und Datalogix, weltweit arbeitet es außerdem auch mit BlueKai, Epsilon und Quantium zusammen. Diese stellen auf Anfrage Zielgruppenlisten zur Verfügung, die Facebook mit seinen Nutzerprofilen abgleicht. Bei Acxiom und Datalogix geschieht das über eine gehashte Mail-Adresse. Facebook erhält also nur Daten über Menschen, die es bereits kennt. Und es gibt nach eigenen Angaben an seine Partner keine personenbezogene Informationen weiter.

Es ist kein Zufall, dass bei externen Daten immer wieder E-Mail-Adressen und Mobilfunknummern eine Rolle spielen. Sie sind die Schlüssel, mit denen Facebook Daten aus fremden Quellen mit seinen eigenen Informationen verknüpft: Die WhatsApp-Nutzungszeiten etwa kann Facebook über die Mobilfunknummer in aller Regel einem bestimmten Nutzer des sozialen Netzwerks zuordnen.

Facebook begnügt sich nicht damit, Daten aus verschiedenen Quellen zu sammeln und zu möglichst genauen Profilen zu aggregieren. Das Unternehmen betreibt vielmehr eine große Datenanalyse-Abteilung, die versucht, den vorhandenen Daten neue Informationen abzuringen. Ab und zu öffnen Facebooks Datenwissenschaftler die Tür zu ihrer Hexenküche einen Spalt und geben Einblick in ihre Forschungen.

Eine komplette semantische Analyse der Beiträge zum Beispiel ist mit dem DeepText-Projekt auf dem Weg. Es soll Facebook-Posts, Kommentare und Nachrichten in über 20 Sprachen verstehen. Dabei soll es neben dem grundsätzlichen Thema auch die Stimmung eines Textes sowie die Ereignisse, Personen und Orte identifizieren, um die es darin geht.

Im Zweifel aggressiv

Ihnen wird sicherlich aufgefallen sein, dass wir in diesem Artikel an etlichen Stellen defensiv formulieren. Die vorsichtigen Formulierungen haben den Grund, dass wir es einfach nicht genauer wissen. So groß das Interesse Facebooks an den Informationen über Dritte sein mag, so zurückhaltend ist es darin, Dinge über sich preiszugeben.

Wir haben Facebook eine Liste mit Fragen geschickt, um genauer zu erfahren, welche Daten das Unternehmen an welchen Stellen einsammelt und was es damit macht. Erhalten haben wir aber nur sehr vage allgemeine Informationen. Ein Stück weit kann man das auch nachvollziehen: Ein Werbekonzern wie Facebook will der Konkurrenz sicher nicht aufs Brot schmieren, wie man Datenberge über Menschen effektiv aufbereitet.

Für Sie bedeutet das, dass Sie unsere Erläuterungen interpretieren müssen. Und dabei sollten Sie eher davon ausgehen, dass Facebook aggressiv alles aufsaugt, was es kriegen kann und damit alle beschriebenen Methoden auf seine Daten loslässt – und womöglich noch ein paar mehr, von denen auch wir noch nichts gehört haben. Daten sind ein wertvoller Rohstoff in der Werbebranche und Facebook ist ein Meister darin, diesen Rohstoff zu raffinieren. *(jo@ct.de)* c't

Weiterführende Informationen:
ct.de/y29a

Außen vor

Daten bei Facebook kontrollieren und löschen

Facebook bietet eine Reihe von Funktionen, mit denen sich gespeicherte Informationen überprüfen und löschen lassen und mit denen man für seine Daten festlegt, wer sie zu sehen bekommt. Man muss die Einstellungen dafür nur finden.

Von Jo Bager

Mache Facebook zu deinem Facebook – Ende Oktober hat Facebook eine millionenschwere Werbekampagne gestartet. Anzeigen in Tageszeitungen, Publikumszeitschriften und Außenwerbung sollen Deutsche davon überzeugen, dass sie jederzeit die Kontrolle darüber haben, was von ihnen bei Facebook zu sehen ist.

In der Tat kann man viele der Dinge kontrollieren, die Facebook über einen weiß und die Dritte zu sehen bekommen. Leider ist es nicht so einfach, wie es die Anzeigen suggerieren. Dort steht zum Beispiel „Ich hab mal etwas gepostet, was ich nie, nie, nie hätte teilen sollen." Als Lösung bietet das Banner an: „Auf Facebook etwas zu löschen heißt: Es ist weg. Schnell und unkompliziert."

Das ist allerdings grob irreführend. Denn wenn etwas erst einmal in einem digitalen Medium wie Facebook veröffentlicht wurde, kann man nie mehr sicherstellen, dass es „weg" ist. Man kann es zwar in seiner eigenen Timeline löschen. Aber andere können es bis dahin kopiert haben und jederzeit wieder veröffentlichen.

Plattformfrage

Deshalb lautet eine gute Faustregel im Umgang nicht nur mit Facebook, sondern mit digitalen Medien generell: Alles, was man veröffentlicht, sollte man auch Fremden auf der Straße zeigen können. Nur wenn man diese Regel immer beherzigt, kann man sicher sein, dass zum Beispiel Fotos, die nur für die Augen enger Freunde bestimmt sind, nicht plötzlich in der Öffentlichkeit auftauchen.

Der Zugriff auf Posts lässt sich in der Facebook-Timeline auf bestimmte Adressaten einschränken. Zudem hält die Plattform auch geschlossene und geheime Gruppen bereit, in denen sich Gleichgesinnte austauschen können, ohne dass Dritte mitlesen. Selbsthilfegruppen zum Beispiel machen davon Gebrauch. Will man über intime oder vertrauliche Dinge kommunizieren, gibt es aber geeignetere Medien, denn Facebook liest immer mit.

Als Alternative bieten sich zum Beispiel Messenger an, die Nachrichten Ende-zu-Ende-verschlüsseln. Dazu gehören etwa Threema und WhatsApp. Denn durch die Verschlüsselung bekommen nur die Teilnehmer einer Konversation die Inhalte zu Gesicht, nicht aber der Plattform-Betreiber. Auch der Facebook Messenger beherrscht Ende-zu-Ende-Verschlüsselung, ist aber zu unflexibel. So lassen sich Chats dort nur von einem bestimmten Gerät zu einem bestimmten anderen verschlüsseln. Im Unterschied zu Threema und WhatsApp erlaubt er zudem keine verschlüsselten Gruppenchats.

Inventur

Im Laufe der Nutzung fallen bei Facebook viele Informationen an, die insgesamt ein recht scharfes Profil Ihrer Persönlichkeit abgeben. Sie sollten sich daher von Zeit zu Zeit einen Überblick über die gespeicherten Daten verschaffen und gegebenenfalls aufräumen. Einen ersten Eindruck über die eigenen Aktivitäten gibt einem das Aktivitätenprotokoll, zu erreichen über den Link im Banner-Bereich des eigenen Profils. Hier listet Facebook

minutiös auf, was man wann gemacht hat. Jeder Eintrag lässt sich einzeln editieren oder löschen.

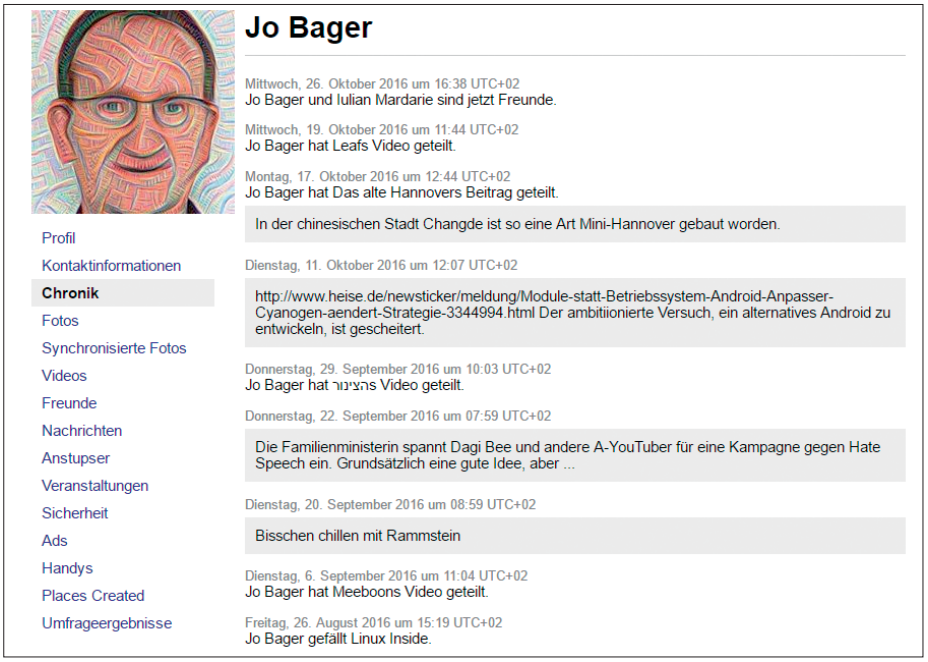
Mit dem Privatsphäre-Check können Sie sich Ihr Profil auch mit den Augen eines anderen Mitglieds ansehen, um zu konktrollieren, dass dieses wirklich nur zu Gesicht bekommt, was es sehen soll. Sie finden ihn über das Schloss-Icon in der Menüleiste. Dort können Sie auch mit „Wer kann meine zukünftigen Beiträge sehen?“ den Standard-Empfängerkreis für das Posten zukünftiger Beiträge vorgeben: „Öffentlich“, „Freunde“, „Nur ich“, oder – oft die beste Wahl – „Weitere Optionen“. Hier können Sie eigene Empfängerlisten definieren.

Sie können sich auch eine Kopie aller persönlicher Informationen, die Sie auf Facebook geteilt haben, erzeugen lassen (alle URLs unter dem c’t-Link). Facebook stellt die Daten als Zip-Datei zum Herunterladen bereit. Das Paket zu schnüren dauert ein paar Minuten. Facebook weist Sie mit einer Mail darauf hin, wenn der Download bereitsteht.

Das Paket gibt Ihnen einen guten Eindruck davon, wie viel Facebook über Sie weiß. Beim Autoren dieses Artikels, wahrlich kein Facebook-Junkie, sind nur an Text-Inhalten 2 MByte zusammengekommen. Das entpackte Download-Paket stellt die Informationen übersichtlich in Form von HTML-Seiten dar, je eine für „Kontaktinformationen“, „Chronik“, „Fotos“, „Nachrichten“ und zehn weitere Kategorien.

Der Download umfasst aber nur Informationen, die Sie selber explizit auf Facebook hochgeladen haben. Facebook weiß aber noch mehr über Sie, zum Beispiel indem es Ihr Verhalten auswertet. Diese Rückschlüsse gehen in Ihr Werbeprofil ein, die Grundlage für Werbung, die Facebook Ihnen präsentiert.

In seinen Werbeeinstellungen zeigt Facebook Interessengebiete an, von denen es glaubt, das sie Sie interessieren. Sie erreichen diese Einstellungen, wenn Sie den Menüeintrag „Warum wird mir das hier angezeigt“ des zu jeder Facebook-Anzeige gehörenden Menüs auswählen und im Pop-up, das dann erscheint, auf „Deine Einstellungen für Werbeanzeigen verwalten“ klicken. Dort können Sie dann Ihr Werbeprofil anpassen – zum Beispiel, indem Sie alle Interessen löschen. Facebook zeigt Ihnen dann weniger relevante Werbung, andere Konsequenzen hat dies nicht.



Facebook stellt eine Kopie aller persönlichen Informationen, die man auf Facebook geteilt haben, als Paket zum Herunterladen bereit.

Im Schaltraum

Weitere den Datenschutz betreffende Optionen finden sich in den Einstellungen. Unter „Privatsphäre“ etwa lässt sich festlegen, wer einen kontaktieren und wer nach einem suchen darf. Möchten Sie die Reichweite sämtlicher alter Beiträge komplett auf die Freunde einschränken, findet Sie dort ebenfalls den Schalter dafür.

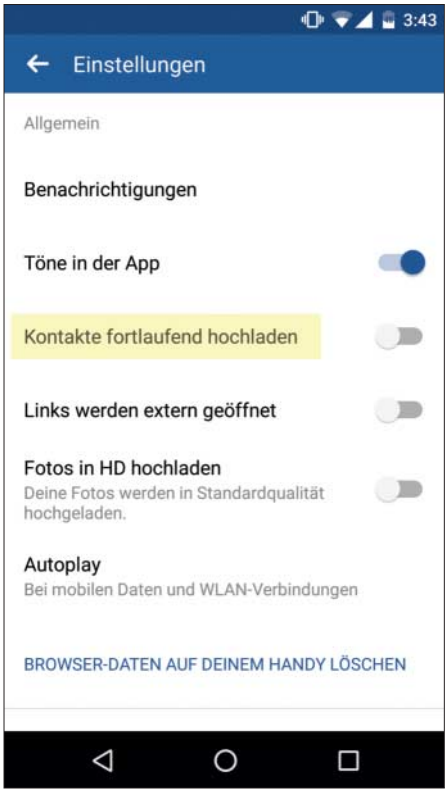
Unter „Chronik und Markierungseinstellungen“ lässt sich feintunen, was für wen in der eigenen Chronik zu sehen sein soll, und wer dort posten darf. Dort legen Sie zum Beispiel fest, dass nur Ihre Freunde in Ihrer Chronik posten dürfen und dass auch nur Sie und Ihre Freunde diese Posts zu Gesicht bekommen – eine solche Einstellung ist immer ganz gut, wenn der Chef die privaten Partyfotos nicht sehen soll, die Freunde in der Timeline posten.

Facebook nutzt Informationen über seine Mitglieder nicht nur selbst, sondern fungiert auch als Plattform für Drittanbieter-Apps – denen es Informationen bereitstellt. Von Zeit zu Zeit sollte man auch in den App-Einstellungen mal nachsehen, wer da eigentlich alles auf welche Daten zugreifen kann, und aufräumen. Unter „Werbeanzeigen“ kommen Sie zu den allgemeinen Werbeeinstellungen, legen fest, ob Sie überhaupt interessenbasierte Anzeigen sehen wollen und ob Facebook Banner mit Ihren sozialen Handlungen verknüpfen darf – ob sich also der Pizzabäcker mit seiner Kampagne für die neue Lasagne auf Ihr „Like“ für Nudelgerichte beziehen darf.

Daten von Dritten

Man gibt Facebook nicht nur Daten über sich selbst. Insbesondere der Freundefinder lädt einen dazu ein, auch Daten über Dritte preiszugeben, indem man sein Adressbuch hochlädt. Die Facebook-Apps für Android und iOS zum Beispiel laden Adressbuchdaten hoch, wenn dort die sogenannte „laufende Synchronisierung“ aktiviert ist.

Unter Android deaktivieren Sie dies in den Optionen unter „App-Einstellungen“, unter iOS unter „Einstellungen\Allgemein“. Dort nennt sich der Schalter „Kontakte hochladen“. Haben Sie bereits Kontakte hochgeladen? Auf der Seite „Einladungen und importierte Kontakte verwalten“ können Sie es kontrollieren – und auch einzelne oder alle importierten Kontakte wieder entfernen.



„Kontakte fortlaufend hochladen" bedeutet: Facebook schaufelt sich alle Adressbucheinträge rein – besser abschalten.

Nach der Lektüre der vorigen beiden Artikel wollen Sie nur noch weg von Facebook und alle Ihre dort gespeicherten Informationen löschen lassen? Das ist möglich, Facebook bietet auch dafür ein Formular. Der Dienst weist darauf hin, dass es nur die selbst geposteten Beiträge löscht. Insgesamt dauert es laut Facebook bis zu 90 Tage, bis alle Inhalte gelöscht sind.

Draußen

Auch wenn Sie nicht bei Facebook sind, sieht das Unternehmen Sie auf jeder Website, welche den Like-Button, andere sogenannte Social Plugins oder Werbung von Facebook anzeigen. Mit einem Cookie kann das Unternehmen alle Seitenaufrufe auf einen Anwender zurückführen. Auch bei Nichtmitgliedern kommen so umfangreiche Profile zusammen.

Sie können dem Unternehmen aber verbieten, Nutzungsdaten für das Targeting zu erheben. Dazu lassen Sie auf www.youronlinechoices.eu ein sogenanntes Opt-out-Cookie setzen. Die Plattform vereint übrigens so ziemlich alle Werbevermarkter, die mit Targeting arbeiten, sodass sie diese Cookies auch für viele andere Werbeunternehmen setzen können.

Die Opt-out-Cookies bewahren Sie aber nicht davor, Werbung angezeigt zu bekommen: Ihre IP-Adresse landet also auf jeden Fall bei Facebook. Abgesehen davon birgt diese Methode das Risiko, dass man die Opt-out-Cookies mitlöscht, wenn man seinen Browser mal aufräumt. Dann muss man sie neu setzen lassen. Nachhaltiger schützen Browser-Add-ons gegen neugierige Anzeigenvermarkter wie Facebook, zum Beispiel Adblocker wie das für Chrome, Safari und Firefox verfügbare uBlock.

Für Android und iOS gibt es ebenfalls Werbeblocker, die neugierige Ausspäher ausperren. Soll Facebook per App den Aufenthaltsort mitloggen? Falls nicht, können Sie mit den Einstellungen des Mobilsystems der Facebook-App und der anderen Apps des Unternehmens das Recht entziehen, auf den Standort zuzugreifen.

Benutzt man Facebooks Login, um sich mit dem Facebook-Account woanders einzuloggen, bekommt das Unternehmen mit, welche Dienste man nutzt und wann. Wer das nicht möchte, muss wohl in den sauren Apfel beißen und sich für Drittanbieterdienste eigene Accounts anlegen beziehungsweise bestehende von Facebooks Login auf herkömmliche Logins umstellen. Mit einem Passwortmanager ist es aber gar nicht so schwierig, auch mit vielen Zugangsdaten zu hantieren.

Als Webmaster stehen Sie vor einem Dilemma: Der Like-Button von Facebook sowie andere Social-Media-Buttons helfen, Ihre Seiten bekannter zu machen. Gleichzeitig melden diese aber die IP-Adresse und gegebenenfalls weitere Nutzerdaten Ihrer Besucher bei jedem Seitenaufruf an Facebook und Co.

c't hat dafür eine Lösung entwickelt. Der c't Shariff ersetzt die Standard-Buttons für das Teilen von Inhalten durch eigene. Shariff-Buttons stellen den direkten Kontakt zwischen Social Network und Besucher erst dann her, wenn Letzterer aktiv auf den Share-Button klickt. Shariff hat sich auf tausenden Websites bewährt und steht als kostenlose Open-Source-Lösung für die verschiedensten Plattformen zum Herunterladen zur Verfügung.

Facebook stellt eine Reihe von Kontroll- und Steuermöglichkeiten für die von seinen Nutzern hochgeladenen Informationen bereit: Wer Facebook verlässt, kann seine Daten wieder löschen lassen; Nichtmitglieder können das Datensammeln für Werbeprofile unterbinden; Webmaster schützen ihre Besucher mit Shariff vor dem neugierigen Like-Button: Ist also alles bestens?

Eher nicht. Die vom Nutzer selbst hochgeladenen Informationen sind nur ein Bruchteil dessen, was Facebook über ihn weiß – siehe auch den Artikel ab Seite 76. Facebook hat also viel mehr Informationen über jeden einzelnen, als alle zur Verfügung stehenden Kontroll- und Löschmechanismen überhaupt erreichen können. Bei der Kontolöschung spricht Facebook explizit nur davon, die vom Nutzer selbst geposteten Beiträge zu löschen.

Und was heißt eigentlich Löschen bei Facebook: Endgültiges Entfernen aus den Datenbanken? Die Recherchen des Datenschützers Max Schrems deuten darauf hin, dass Facebook Inhalte möglicherweise gar nicht endgültig löscht, sondern nur mit einem Löschvermerk versieht.

Wir wissen nicht, wie genau Facebook mit Ihren Daten verfährt. Das Unternehmen ist bei solchen Informationen zu sich selbst sehr zurückhaltend. In den USA gibt es keine Aufsichtsbehörde, die die Datensammelei effektiv kontrolliert und im Zaum hält.

Nur Druck hilft

Wann immer deutsche Datenschützer mehr herausfinden oder die Datengier bremsen wollen, versucht Facebook, sich mit vielfältigen juristischen Winkelzügen zu entziehen. Dazu gehört das Argument, die irischen, nicht die deutschen Datenschützer seien in der EU für Facebook zuständig, weil Facebook seinen EU-Hauptsitz in Irland hat. Die irische Behörde wiederum hat sich in der Vergangenheit im Umgang mit Facebook als überforderter, zahnloser Tiger erwiesen.

Es gibt wohl nur einen Weg, Facebook zu mehr Transparenz und Datenschutz zu bewegen: Man muss das Unternehmen vor Gericht dazu zwingen. Der folgende Artikel fasst die derzeitig gegen Facebook angestrengten Verfahren zusammen.

(jo@ct.de) c't

Weiterführende Informationen:
ct.de/ym9z

Brüchiges Recht

Wie schwer es ist, Datenschutzverstöße von Facebook juristisch zu ahnden

Es ist kein Geheimnis, dass Facebook in seiner Datenspeicherwut oft den rechtlich sauberen Bereich verlässt. Permanent liegt der US-Konzern im Clinch mit europäischen Datenschutzbehörden und Verbraucherschützern. Viel mehr als kleine Nadelstiche konnten die Gegner allerdings bislang nicht setzen – was auch an Facebooks Verteidigungstaktik liegt.

Von Holger Bleich

Die einen sehen in Prof. Johannes Caspar den Don Quijote, der einen aussichtslosen Kampf gegen die Datenkraken führt. Andere verspotten ihn als Datenschutz-Taliban, der den digitalen Fortschritt behindert. Caspar hat es nicht leicht als Hamburgischer Beauftragter für den Datenschutz: Mit Facebook und Google haben die zwei größten Internet-Konzerne ihren deutschen Sitz in Hamburg – unterliegen also zuständigkeitshalber seiner Aufsicht.

Google gibt sich mittlerweile vergleichsweise transparent und kooperativ. Ganz anders dagegen Facebook – immer wieder beharkt Caspar den US-Konzern im Interesse der deutschen Verbraucher. Jüngstes Beispiel: Ende September hat er eine Verwaltungsanordnung erlassen, die es Facebook untersagt, Daten von deutschen Nutzern des Tocherunternehmens WhatsApp zu erheben und zu speichern. Außerdem soll Facebook bereits übermittelte Daten löschen. Eine solche Anordnung ist die Voraussetzung dafür, dass die Behörde gegen Facebook klagen kann.

Facebook beugt sich nach eigenen Angaben dieser Anordnung, hat aber bereits beim Verwaltungsgericht Hamburg einen „Antrag auf Aussetzung der sofortigen Vollziehbarkeit der Verwaltungsanordnung“ gestellt – mit dem üblichen Argument: Deutsches Datenschutzrecht gelte für Facebook nicht, weil sich der europäische Hauptsitz des Konzerns im Dublin befinde. Deshalb sei die irische Datenschutzaufsicht zuständig.

In Deutschland ist Facebook durch die Facebook Germany GmbH in Hamburg vertreten, die sich vornehmlich um deutsche Reklame auf der Plattform kümmert, nicht aber um die strittige Datenverarbei-

tung. Dafür sei die Facebook Ireland Ltd. zuständig, und deshalb sei deutsches Datenschutzrecht nicht anwendbar, urteilten sowohl das Oberverwaltungsgericht Schleswig (Az. 4 MB 10/13) als auch das Verwaltungsgericht Hamburg (Az. E 4482/15). Hierbei ging es ebenfalls um eine Verordnung Caspars. Er wollte Facebook verpflichten, in Deutschland Nutzer-Pseudonyme zuzulassen und dauerhaft auf die Klarnamenpflicht zu verzichten. Das Gericht ist der Ansicht, dass deutsches und irisches Datenschutzrecht miteinander konkurrieren. In einem solchen Fall sei das Recht desjenigen Landes anzuwenden, in dem sich die Niederlassung mit der engsten Verbindung zur streitigen Datenverarbeitung befindet – im Falle von Facebook eben Irland. Gegen den Beschluss ging Caspar in Berufung, eine Entscheidung des Oberverwaltungsgerichts Hamburg steht noch aus.

Zuständigkeits-Wirrwarr

Unterdessen beschäftigt diese verzwickte deutsche Rechtslage sogar den Europäischen Gerichtshof (EuGH): Das Kieler Unabhängige Landeszentrum für Datenschutz (ULD) treibt seine Klage gegen die Betreiberin einer Facebook-Fanpage seit 2011 durch die Instanzen. Laut ULD erhebt Facebook auf den Fanpages über ein Cookie Nutzerstatistiken, ohne sich eine Einwilligung dafür geholt zu haben. Die Sache liegt derzeit beim Bundesverwaltungsgericht in Leipzig, das nicht entscheiden will, ohne zuvor die Meinung des EuGH zu europarechtlichen Aspekten erfahren zu haben.

Deshalb befragte es im Februar 2016 den EuGH, ob die deutsche Facebook-Niederlassung in die Pflicht genommen werden kann. Mit einer Entscheidung des obersten europäischen Gerichts in dieser so wichtigen Frage ist wohl erst 2017 zu rechnen. Sie könnte allerdings bereits 2018 wieder obsolet werden, wenn die neue EU-Datenschutz-Grundverordnung (DSGVO) in Kraft tritt.

Facebook-Spam

Nicht nur die Datenschutz-Aufseher, sondern auch deutsche Verbraucherschutz-Organisationen gehen immer wieder gegen die überbordende Sammelwut Facebooks juristisch vor.

Im Januar 2016 bestätigte der Bundesgerichtshof (BGH), dass Facebook für eigene Rechtsverstöße auf der Plattform haftet (Az. I ZR 65/14). Allerdings ging es nur mittelbar um Fragen des Datenschutzes: Der Verbraucherzentrale Bundesverband (vzbv) ist 2011 gegen die Funktion „Freunde finden“ in ihrer Ausgestaltung vom Herbst 2010 vorgegangen. Hatte ein Facebook-Mitglied sie genutzt, übergab er oder sie seine Adressbuchdaten an Facebook. Das soziale Netzwerk durchsuchte die Daten dann aber nicht nur nach registrierten Mitgliedern, sondern verschickte auch Einladungen an nicht registrierte Bekannte.

Das Safe-Harbor-Abkommen kippte aufgrund Facebooks Sammelwut.

Der BGH bestätigte in letzter Instanz ein Urteil des Kammergerichts (KG) Berlin, wonach Facebook seine Mitglieder nicht über die Auswertung der importierten Daten aufgeklärt und Einladungs-Mails auch an Nichtmitglieder verschickt hat. Im Klartext: Der BGH stellte fest, dass Facebook nach allen Regeln der Kunst massenhaft gespammt hat. Zuvor hatte das KG Berlin in seinem Urteil zusätzlich angemerkt, dass die Datenverarbeitung bei Facebook faktisch nicht in Irland, sondern in den USA erfolgt (Az. 5 U 42/12). Die Daten habe der Konzern in Deutschland erhoben, weshalb hiesiges Datenschutzrecht anzuwenden sei.

Like-Schnüffelei

Besonders aufsehenerregend war aber ein Urteil des Landgerichts (LG) Düsseldorf im März 2016 (Az. 12 O 151/15). Es dehnte die datenschutzrechtliche Haftung von Facebook sogar auf deutsche gewerbliche Kunden des sozialen Netzwerks aus. Die Verbraucherzentrale NRW hatte die Unternehmen HRS, Nivea (Beiersdorf), Payback, Eventim, Fashion ID und kik abgemahnt, weil sie per Social-Plug-in Facebooks Like-Button in ihre Websites eingebunden hatten (Page-Plug-in).

„Bei direkter Einbindung der Gefällt-mir-Schaltfläche liest der soziale Netzwerk-Gigant schon bei jedem bloßen Aufruf der jeweiligen Seiten automatisch mit“, monierte die Verbraucherzentrale. Das passiere „unabhängig davon, ob der Seitenbesucher Facebook-Mitglied ist oder nicht.

Die Verbraucherzentrale verlangte von den Unternehmen, sich vor der Datenweitergabe an Facebook eine aktive Einwilligung einzuholen – wie es etwa das quelloffene c’t-Projekt „Shariff“ realisiert. Vier der abgemahnten Unternehmen hatten daraufhin eine Unterlassungserklärung abgegeben. Da sich Payback und die Peek&Cloppenburg-Tochter Fashion ID weigerten, reichte die Verbraucherzentrale NRW Klage gegen die beiden Unternehmen an den Landgerichten Düsseldorf und München ein.

Das LG Düsseldorf untersagte Fashion ID tatsächlich die Nutzung des Page-Plug-ins von Facebook. Laut Gericht sind IP-Adressen der Besucher von Webseiten, die ein Page-Plug-in enthalten, personenbezogene Daten und fallen deshalb unter die Einwilligungspflicht nach dem Bundesdatenschutzgesetz (BDSG). Die Richter hoben darauf ab, Facebook habe so viele andere personenbezogene Daten von Mitgliedern und Nicht-Mitgliedern, dass es schon deshalb fast jede hinterlassene IP-Adresse mit persönlichen Daten verknüpfen kann.

Das Urteil hat zu heftigen Kontroversen unter Datenschutzexperten geführt. Obwohl der Website-Betreiber die Daten nicht selbst erhebt, sondern lediglich für Facebook „beschafft“, gilt er für das LG Düsseldorf als „verantwortliche Stelle“ im Sinne des BDSG. „In vielerlei Hinsicht lässt einen die Begründung des Gerichts zumindest innehalten oder die Stirn runzeln“, konstatierte Datenschutzexperte Dr. Carlo Piltz. „Möchten Webseitenbetreiber die durch das Gericht aufgestellten Voraussetzungen erfüllen und dabei nicht auf Lösungen wie die 2-Klick-Lösung zurückgreifen, bleibt wohl nur ein Popup oder Banner, welcher eine Einwilligungserklärung mit Opt-in-Checkbox enthält.“

Das Urteil beschränke sich nicht alleine auf das Page-Plug-in, „sondern betrifft Like-Buttons, andere Social-Plug-ins und praktisch das ganze dynamische Internet“, kommentierte Dr. Thomas Schwenke, Anwalt und Experte für Social-Media-Recht. Denn die Einbindung fremder Inhalte, Skripte oder Dienste setze voraus,

Bild: europe-v-facebook.org

Datenschützer Max Schrems besucht den Hauptsitz der irischen Datenschutzaufsicht (hinten).

dass deren Lieferanten die IP-Adresse der Website-Besucher kennen, um die Inhalte übermitteln zu können. Alternativ müssten diese Anbieter auf die Erfassung der Daten verzichten. „Dies klingt radikal, aber letztendlich ist es das, was die Datenschützer fordern“, resümierte Schwenke.

Noch ist das endgültige Urteil nicht gesprochen. Nach Informationen von c’t hat Facebook gegen die LG-Entscheidung Berufung eingelegt. Sie ist also nicht rechtskräftig. Derzeit läuft das Verfahren am Oberlandesgericht Düsseldorf (Az. I/20 U 40/16).

Das Ende von Safe Harbor

Die größten juristischen Schwierigkeiten bei der Datensammelei bereitet Facebook derzeit der österreichische Datenschutz-Aktivist Max Schrems (europe-v-facebook.org). Im Oktober 2015 brachte er nach einer Auseinandersetzung mit der irischen Datenschutzbehörde zur Datentransfer-Praxis von Facebook mit einer daraus resultierenden Klage vor dem EuGH das Datentransfer-Abkommen Safe Harbor zwischen der EU und den USA zu Fall.

Das höchste europäische Gericht folgte seiner Argumentation: Der erlaubte Zugriff von Behörden auf Nutzerdaten in den USA verletze „den Wesensgehalt des Grundrechts auf Achtung des Privatlebens“. US-Unternehmen wie Facebook seien verpflichtet, in Europa geltende Schutzregeln außer Acht zu lassen, wenn US-Behörden aus Gründen der nationalen Sicherheit beziehungsweise des öffentlichen Interesses Zugriff auf persönliche Daten verlangen.

Ab diesem Zeitpunkt war es Facebook und anderen US-Konzernen de facto zwar untersagt, personenbezogene Daten europäischer Nutzer in die USA zu transferieren und dort zu verarbeiten. Aber ändern mussten sie nichts, weil freilich zeitlich begrenzte Alternativ-Regelungen geschaffen wurden. Dennoch: Schrems hat die EU dazu gezwungen, sehr zügig ein Nachfolge-Abkommen mit den USA auszuhandeln. Herausgekommen ist das mittlerweile in Kraft getretene „EU-US Privacy Shield“.

Dieses Abkommen steht schon jetzt auf wackeligen Beinen, und zwar wieder aus den gleichen Gründen. Viele Experten halten es für angreifbar. Schrems hat bereits angekündigt, auch gegen diese Nachfolge-Regelung vorgehen zu wollen. Die Nichtregierungsorganisation Digital Rights Ireland hat derweil schon Nägel mit Köpfen gemacht und im Oktober Klage am EuGH gegen Privacy Shield eingereicht (Az. T-670/16). Ziel sei die Annullierung des Abkommens, teilte die Organisation mit. Derzeit überprüft der EuGH, ob die Klage zulässig ist.

US-Konzerne wie Google und Microsoft haben sich mittlerweile dem neuen Abkommen unterworfen. Ausgerechnet Facebook aber hat sich lange geziert. Mitte Oktober war es dann soweit, allerdings Facebook-typisch mit Einschränkungen: Facebook beugt sich dem Abkommen nur für das Produkt „Workplace by Facebook“ und für den Geschäftsbereich Werbeanzeigen. Ob der Konzern deshalb Ärger von europäischen Datenschutzbehörden bekommt, ist noch unklar.

Datenschutz-Sammelklage

Längst hat Schrems eine zweite juristische Front gegen Facebook aufgemacht: Auf der Website fbclaim.com überzeugte er rund 25.000 Facebook-Nutzer, ihn zu einer Sammelklage gegen Facebook zu ermächtigen. Mittlerweile liegt die Sache höchstinstanzlich beim österreichischen Obersten Gerichtshof (OGH). Schrems wirft Facebook unter anderem „die Verwendung ungültiger Datenschutzbestimmungen, die unrechtmäßige Verarbeitung und Weitergabe von Daten und die Teilnahme an US-Massenüberwachungsprogrammen“ vor. Er fordert in der Klage von Facebook pro Betroffenem einen symbolischen Schadenersatz von 500 Euro.

Facebook reagierte wie so oft nicht inhaltlich, sondern bringt bislang lediglich formelle Argumente in Stellung: Der US-Konzern bestreitet, dass der OGH für die Entscheidung in diesen Datenschutzfragen zuständig ist. Außerdem sei Schrems durch die mediale Berichterstattung und seine Vorträge zum Thema Datenschutz nicht mehr als „Verbraucher“ zu sehen und dürfe daher nicht mehr an seinem Heimatort Wien klagen.

Facebook bezweifelt, dass eine Sammelklage von Verbrauchern aus aller Herren Länder überhaupt zulässig ist, wenn diese ihre Ansprüche an einen anderen Verbraucher übertragen. Damit steht der Konzern nicht allein: Das Landesgericht für Zivilrechtssachen in Wien hatte die Klage in erster Instanz nicht zugelassen. Das Oberlandesgericht hat 20 der 22 Punkte als zulässig befunden, aber eine Sammelklage abgelehnt.

Der OGH ist sich in dieser Frage offenbar noch unschlüssig. Und deshalb landet „Schrems gegen Facebook“ wieder mal beim EuGH: Am 12. September reichte der OGH die Entscheidung nach Luxemburg weiter. Er möchte vom EuGH wissen, ob Schrems’ Sammelklage gegen die Datensammelei von Facebook mit Europarecht vereinbar ist.

Mit einer Entscheidung des obersten europäischen Gerichts ist frühestens 2017 zu rechnen. Sollte sich Schrems durchsetzen, würde er endgültig zum personifizierten Albtraum für Facebook – Datenschutz-Sammelklagen gegen den US-Konzern wären Tür und Tor geöffnet. Schrems sieht sich im Vorteil: „Der EuGH war bisher durchaus verbraucherfreundlich, wenn es um den Gerichtsstand ging. Wenn man es nüchtern betrachtet, gibt es wenig gute Gründe, die gegen uns sprechen – aber es wird jedenfalls spannend.“ *(hob@ct.de)* c't