Innovation und Datenschutz – kein Widerspruch

74

Raoul-Thomas Herborg und Doris Hausen

Zusammenfassung

Smartphones und Tablets eröffnen für Unternehmen eine Vielzahl neuer Geschäftsfelder und Dienste. Diese basieren auf der permanenten Verfügbarkeit der Geräte beim Anwender und der umfassenden Sensorik. Dadurch wird es möglich, eine Vielzahl sensibler Daten von Personen zu erfassen, mit potentiell gravierenden Auswirkungen auf die Privatsphäre des Anwenders. Dieser Artikel beleuchtet die Themen Datenschutz und Datensicherheit im Umfeld mobiler Dienste und gibt Unternehmen praxisbezogene Handlungsempfehlungen bei der Entwicklung mobiler Dienste. Der Schutz sensibler Daten muss bei der Gestaltung neuer Dienstleistungen und Geschäftsfelder von Anfang an berücksichtigt werden, damit diese langfristig erfolgreich sind.

74.1 Einführung

Der Einsatz von Smartphones und Tablets wächst rasant und verändert die Art, wie wir unser Leben organisieren, wie wir kommunizieren und wie wir arbeiten fundamental. Diese Geräte bieten eine Vielzahl an Funktionen und Möglichkeiten, die sie für viele Menschen zum unverzichtbaren und immer verfügbaren Begleiter gemacht haben.

R.-T. Herborg (✉) · D. Hausen
virtual solution AG, München, Deutschland
E-Mail: raoul.herborg@virtual-solution.com

D. Hausen
E-Mail: doris.hausen@virtual-solution.com

C. Linnhoff-Popien et al. (Hrsg.), *Marktplätze im Umbruch,* Xpert.press,
DOI 10.1007/978-3-662-43782-7_74

Die grundlegende Veränderung besteht einerseits in der permanenten Verfügbarkeit dieser Geräte beim Anwender, andererseits in der immer umfangreicher werdenden Sensorik, die vollkommen neue Anwendungen ermöglichen.

Noch nie konnten Privatpersonen, Kunden, Geschäftspartner und Unternehmen jederzeit so umfassend miteinander kommunizieren. Dies reicht von der simplen Bereitstellung von Informationen bis hin zu einer tiefen Integration von komplexen Prozessen. Die in Mobilgeräten verbauten Sensoren können dazu eine Vielzahl an relevanten Informationen bereitstellen: Vom aktuellen Aufenthaltsort des Nutzers über Audioaufnahmen, Fotos und Videoaufnahmen der Umgebung, bis hin zu persönlichen Details über Vitalfunktionen der Person.

Das Mobilgerät entwickelt sich damit zur Datendrehscheibe und Steuerzentrale des persönlichen Umfeldes und damit letztlich zum zentralen Gateway zwischen Menschen und der digitalen Welt. Für Unternehmen eröffnet dies völlig neue Geschäftsfelder und Märkte. Ganze Branchen werden durch neuartige Dienstleistungen wie etwa dem Taxi-Service Uber[1] in Frage gestellt. Richtig genutzt eröffnen sich durch diese Digitalisierung der Gesellschaft heute noch kaum absehbare Chancen und Möglichkeiten, allerdings mit drastischen Auswirkungen bezüglich Datenschutz und Datensicherheit.

Das omnipräsente Mobilgerät eröffnet Zugang zu Informationen des Anwenders, die tief in seine Privatsphäre reichen und die der Anwender – anders als am PC – häufig unbewusst zur Verfügung stellt. So zeichnen unverdächtige Anwendungen auf Mobilgeräten, wie die Flashlight App[2] von iHandy inc. oder das einfache Fruit Ninja Spiel von Halfbrick Studios[3] eine Vielzahl an Daten zu Position, Nutzung des Mobilgeräts, getätigter Anrufe und mehr auf. Diese Daten werden unter anderem an Flurry, ein Tochterunternehmen von Yahoo verkauft. Flurry erstellt basierend darauf detaillierte Benutzerprofile und gibt selbst an, pro Tag 2 Terrabyte an Daten aus 2,8 Mio. App-Nutzungen zu sammeln [10].

Unternehmen stehen vor der Herausforderung zu entscheiden, wie sie mit den Themen Datenschutz und Datensicherheit bei der Entwicklung von mobilen Diensten umgehen.

74.2 Datenschutz und Datensicherheit – Eine Einordnung

Die allgemeine Wahrnehmung, dass das Thema Datenschutz und Datensicherheit derzeit für Anwender wenig Relevanz besitzt, wird in Studien bestätigt [11]. Bisher hat sich gezeigt, dass kein signifikanter Zusammenhang zwischen der persönlichen Einstellung einer Person zum Datenschutz und dem tatsächlichen Handeln besteht. Auch sogenannte *Privacy Fundamentalists* [6], die in Studien angeben, dass ihnen das Thema Datenschutz sehr wichtig ist, teilen sehr sensible Informationen über soziale Netzwerke wie Facebook, das sogenannte „Privacy Paradoxon“. Das trifft auch in dem Fall zu, wenn Anwendern reale

[1] http://www.uber.com (Letzter Aufruf: 1.10.2014).

[2] http://www.fastcompany.com/3023042/fast-feed/this-popular-flashlight-app-has-been-secretly-your-sharing-location-and-device-id (Letzter Aufruf: 1.10.2014).

[3] http://www.julianevansblog.com/2011/11/free-mobile-apps-collecting-your-device-data.html (Letzter Aufruf: 1.10.2014).

Szenarien aus Datenschutzvorfällen aufgezeigt werden, wie in der Studie von Woodruff et al. [11]. Die einzig belegbare Auswirkung auf den Umgang mit persönlichen Daten lässt sich für Personen nachweisen, die einen Vorfall bzgl. Privatsphäre hatten, diese ändern tatsächlich ihr Verhalten [11].

Dabei ist davon auszugehen, dass Nutzer von mobilen Endgeräten sich keineswegs bewusst sind, wie viele Rückschlüsse sich basierend auf den erfassten Daten auf persönliches Umfeld, Lebensumstände, Gesundheit und Gewohnheiten ziehen lassen [11]. Allein anhand der zeitbezogenen Erfassung von Geodaten kann abgeleitet werden, welcher beruflichen Tätigkeit eine Person nachgeht, ob sie sich viel in Bars und Diskotheken aufhält und damit möglicherweise regelmäßig Alkohol konsumiert, an welchen politischen oder religiösen Veranstaltungen sie teilnimmt, regelmäßig Sport treibt, oder – in Kombination mit den Daten anderer Nutzer – welche anderen Personen sie wann und wie oft trifft.

Noch weiter in die Privatsphäre des Einzelnen reicht der aktuelle Trend *Quantify Yourself*, wobei umfassend Gesundheitsdaten insbesondere über mobile Endgeräte erfasst werden. So hat Apple mit seiner letzten Softwareaktualisierung iOS 8 eine zentrale App zur Speicherung einer Vielzahl von Daten zu Körper, Gesundheit, Vorerkrankungen und Fitnessaktivitäten entwickelt, die diese Daten – so die Ankündigung – auch mit anderen Apps und Zubehörgeräten austauscht. Mit der für 2015 angekündigten Apple Watch[4] ist es etwa möglich jederzeit Pulsinformationen aufzuzeichnen und in dieser App zu verwalten. Für private Krankenversicherungen würden solche Daten einen erheblichen Wert darstellen, basiert doch deren Erfolgsmodell für niedrigere Krankenkassenprämien – so zumindest eine häufige Unterstellung – im Wesentlichen auf der gezielten Auswahl der Versicherten.

Nicht nur Unternehmen sind potentielle Nutzer dieser Informationen. Auch Staaten sammeln in bis vor kurzem kaum vorstellbarer Weise Daten, wie die Enthüllungen des ehemaligen Mitarbeiters des US-amerikanischen Geheimdienstes Edward Snowden gezeigt haben. Diese Informationen werden, so die offizielle, schwer zu überprüfende Aussage, mit dem klaren Ziel der Terrorabwehr durch staatliche Stellen gesammelt. Dadurch werden Eingriffe des Staates für den einzelnen Bürger, solange er in einer rechtsstaatlichen Demokratie lebt, nur in Einzelfällen als Bedrohung wahrgenommen. In anderen Ländern kann dies aber durchaus eine reale Gefahr darstellen, wie der mutmaßliche Hackerangriff auf Apple-Handys von Demonstranten in Hongkong zeigt[5].

Anders als von George Orwell in seinem Roman „1984“ prognostiziert, erfolgen die umfassendsten Datensammlungen heute in erster Linie nicht durch staatliche Institutionen sondern durch die großen Internetkonzerne. Die prägnanteste Beschreibung dazu liefert Google Gründer Eric Schmidt selbst, mit seinem mittlerweile legendären Satz aus dem Jahre 2010: „Wenn es etwas gibt, von dem Sie nicht wollen, dass es irgendjemand erfährt, sollten Sie es vielleicht gar nicht erst tun.“[6]. Gab es bei der Volkszählung 1987

[4] http://www.apple.com/de/watch/ (Letzter Aufruf: 1.10.2014).

[5] http://www.spiegel.de/netzwelt/netzpolitik/protest-in-hongkong-hacker-greifen-handys-von-demonstranten-an-a-994747.html (Letzter Aufruf: 1.10.2014).

[6] Spiegel 2/2010 http://www.spiegel.de/spiegel/print/d-68621901.html (Letzter Aufruf: 1.10.2014).

noch deutschlandweite Proteste und Boykottaufrufe, wurde die europaweite Volkszählung 2011 (in Deutschland Zensus 2011) weitgehend ohne öffentlichen Widerstand durchgeführt, was auch auf eine veränderte Wahrnehmung bzgl. einer potentiellen Bedrohung der Privatsphäre durch den Staat im Gegensatz zu Organisationen, wie Google, Facebook, Amazon und anderen hindeutet.

Eine weitere Bedrohung die aus der Preisgabe persönlicher Informationen entsteht, sind kriminelle Handlungen. Die Liste der Hackerangriffe mit einer Kompromittierung persönlicher Daten ist lang: „Datendiebstahl bei eBay“, „Bankdaten von zwei Millionen Vodafone-Kunden gestohlen“, „Daten von Millionen Sony-Kunden sind in die Hände von Kriminellen gefallen“, „Millionen Kundendaten bei T-Mobile gestohlen“, … Gerade wenn es um zahlungsrelevante Informationen geht, kann das zu drastischen Auswirkungen für den Anwender führen. Der Skandal mit gestohlenen und im Internet veröffentlichen Nacktbildern prominenter Persönlichkeiten macht das ebenso deutlich, wie das Beispiel gehackter Webcams, über die Benutzer erpresserische Mails mit Fotos von sich selbst erhalten.

Nach Krasnova et al. [5] sorgen sich Nutzer sozialer Netzwerke neben organisatorischen Bedrohungen aber insbesondere vor Auswirkungen im persönlichen Umfeld. Nutzer sozialer Netzwerke erhalten mittlerweile häufig Einladungen vermeintlicher Freunde über deren gestohlene Identitäten zu bestimmten Seiten oder Aktivitäten, häufig mit dem Ziel das Gerät mit Viren, Trojanern oder Dialern zu manipulieren. Auch hat wohl jeder Email-Nutzer bereits Spam-Mails über gehackte Email-Konten von Personen aus dem eigenen Umfeld erhalten, sehr unangenehm für den Eigentümer des kompromittierten Kontos.

Diese und weitere Beispiele machen deutlich, dass Datenschutz und Datensicherheit in einem Zusammenhang stehen. Datensicherheit ist die Basis von Datenschutz, denn ohne Datensicherheit kann nicht garantiert werden, dass Datenschutzvorgaben durchgesetzt werden [8]. Andererseits schafft Datensicherheit alleine noch keinen Datenschutz. Beide Themenbereiche werden im Folgenden betrachtet.

74.3 Datensicherheit

Datensicherheit ist ein sozio-technisches Problem, dass von technischen und organisatorischen Maßnahmen sowie dem persönlichen Verhalten abhängt. Sicherheit ist eine Kette, immer nur so stark, wie ihr schwächstes Glied [9].

Der IT-Grundschutzkatalog des Bundesamtes für Sicherheit in der Informationstechnologie (BSI) bietet eine umfassende Strukturierung möglicher Bedrohungen im IT-Umfeld. Dabei gibt es auch Empfehlungen für den Einsatz von mobilen Geräten [2]. Diese sind sehr detailliert und richten sich klar an Experten in IT-Sicherheit. Zusammengefasst bestehen zur Absicherung von Diensten auf Smartphones aus technischer Sicht insbesondere folgende Herausforderungen:

74.3.1 Identität des Benutzers

Ein wesentlicher Baustein für Datensicherheit ist die eindeutige Identifizierung des Benutzers. Man muss wissen, wer auf bestimmte Informationen und Anwendungen zugreift. Diese sogenannte Authentifizierung erfolgt bei den meisten Geräten über eine PIN, die etwa bei der Aktivierung des Gerätes eingegeben werden muss.

Kennt ein Angreifer diese PIN, hat er vollen Zugriff auf das System. Aber auch ohne vorherige Kenntnisse kann ein vierstelliger PIN in weniger als 40 Min. identifiziert und damit voller Zugriff auf das Gerät erlangt werden[7]. Dabei wird am Telefon selbst oder dem Betriebssystem nichts verändert, d. h. der Einbruch bzw. auch der Datendiebstahl ist für den Besitzer des Gerätes nicht nachvollziehbar. Die auf Android-Geräten übliche Anmeldung über Sperrmuster lässt sich über eine sogenannte „Smudge-Attack“ einfach aushebeln: Das Wischen der Finger beim Verfolgen des Sperrmusters hinterlässt ein eindeutiges Muster auf dem Bildschirm, das sich bei passendem Lichteinfall einfach identifizieren lässt.

Weitere Maßnahmen moderner Smartphones, wie etwa Gesichtserkennung oder Fingerabdruckscanner bieten keine zusätzliche Sicherheit. Diese sollen vielmehr jenen Benutzern ein Mindestmaß an Sicherheit bieten, denen selbst eine PIN-Eingabe zu aufwendig ist und die ihr Gerät ohne jede Authentifizierung einsetzen. Das wird dadurch deutlich, dass diese lediglich zusätzliche Verfahren für die Authentifizierung sind. Entsprechend gibt der Nutzer beim Neustart eines iPhone 5s und höher zunächst die PIN ein, um damit den Fingerabdruckscanner zu aktivieren.

74.3.2 Sicherheit der Daten

Die auf dem Gerät lokal vorhandenen Daten müssen vor unbefugtem Zugriff geschützt sein. Dies gilt unabhängig davon ob ein zufälliger Finder oder ein Dieb das Gerät in den Händen hält, also physikalisch darauf Zugriff hat oder ein Angreifer auf anderem Wege, etwa einer manipulierten App, versucht Daten zu kompromittieren.

Die bestehenden Sicherheitsmaßnahmen von Smartphones werden dabei immer wieder von Angreifern ausgehebelt. So wurden durch das Fraunhofer Institut auch für das verglichen mit anderen mobilen Betriebssystemen relativ sicher geltende Apple iOS immer wieder erhebliche Sicherheitsmängel in wichtigen Sicherheitselementen wie der iOS Keychain nachgewiesen [4]. Das ist die Stelle im Mobilgerät, die sensible Schlüsselinformationen des Benutzers und damit zentrale Sicherheitsmerkmale enthält.

[7] http://www.elcomsoft.com/eift.html (Letzter Aufruf: 1.10.2014).

74.3.3 Sichere Kommunikation

Mobile Endgeräte dienen in allererster Linie der Kommunikation. Neben der naheliegenden Sprachkommunikation oder dem Austausch von Emails, tauschen sowohl das Betriebssystem als auch praktisch alle Apps Daten mit den Backendsystemen der Anbieter dieser Dienste aus[8]. D. h. neben den lokal vorhandenen Daten muss auch die Kommunikation abgesichert werden, sowohl um die übertragenen Daten zu schützen, als auch um sicherzustellen, dass ein kompromittierter mobiler Datenkanal keinen unbefugten Zugriff auf das Geräte oder die Systeme beim Anbieter der Dienste ermöglicht.

74.3.4 Handlungsempfehlung

Aus den dargestellten, wesentlichen technischen Herausforderungen ergibt sich eine Vielzahl weiterer Bedrohungsszenarien, denen mit einem ganzen Bündel an Maßnahmen begegnet werden kann und muss. So gibt es innovative Ansätze, um PIN-Eingaben durch sicherere und gut zu bedienende Lösungen zu ersetzen [12]. Secure Container Lösungen erlauben es Informationen sicher auf dem Gerät abzulegen. Eine echte Ende-zu-Ende Verschlüsselung, möglichst zertifikatsbasiert, macht es Angreifern schwer die Kommunikation zu kompromittieren und damit sensible Daten auf dem Gerät oder den Systemen des Dienstanbieters zu entwenden. Einen guten Einstieg in Bedrohungen und wichtige technische Sicherheitsmaßnahmen bietet das OWASP Mobile Security Project[9], das analog zum Open Web Application Security Projekt für Webanwendungen Handlungsempfehlungen für die Entwicklung von sicheren mobilen Diensten gibt.

Bei der Umsetzung von Sicherheitsanforderungen muss der Anwender stets im Mittelpunkt stehen und eine hohe Benutzerfreundlichkeit erreicht werden. Sicherheitsmaßnahmen sollten Nutzern die Interaktion mit mobilen Geräten nicht erschweren. Nur wenn es Anbietern von Diensten gelingt, eine hohe Sicherheit bei gleichzeitig hoher Benutzerfreundlichkeit zu erreichen, werden diese erfolgreich sein.

74.4 Datenschutz

Die Wahrnehmung, welche Daten schützenswert sind, verändert sich über die Zeit und hängt immer auch vom Kontext ab in dem diese verwendet werden. Allgemein wird unter Datenschutz das Recht auf informelle Selbstbestimmung verstanden. Konkret, dass der Einzelne oder eine Organisation selbst entscheidet, wem welche Daten zu welchem Zeit-

[8] http://www.aisec.fraunhofer.de/de/medien-und-presse/pressemitteilungen/2014/20140403_10000_apps.html (Letzter Aufruf: 1.10.2014).

[9] https://www.owasp.org/index.php/OWASP_Mobile_Security_Project (Letzter Aufruf: 1.10.2014).

punkt und in welchem Kontext zugänglich gemacht werden, wie diese gespeichert, weiterverarbeitet und möglicherweise an Dritte weitergegeben werden [8].

Das steht in starkem Widerspruch zur gängigen Praxis auf mobilen Endgeräten, die dem Anwender genau diese Möglichkeit nicht geben. Hintergrund ist das derzeit verbreitete Geschäftsmodell, dass Leistungen durch den Anwender nicht mit Geld, sondern mit persönlichen Daten bezahlt werden. Dazu trägt vermutlich die Umsonst-Kultur des Internets bei, die Bereitschaft für Dienste zu bezahlen ist häufig gering. 2013 waren 90 % der Apps im Apple App-Store kostenlos, der Durchschnittspreis einer App betrug unter Berücksichtigung der kostenlosen Apps 19 US$-Cent, immer noch mehr als das Dreifache der durchschnittlich 6 US$-Cent im Android App-Store Google Play[10].

Die Erkenntnis, dass der Anwender nicht der Kunde von Google ist, sondern das Produkt, dessen Daten genutzt werden, um Leistungen an Werbekunden zu verkaufen, setzt sich langsam durch. Lanier schlägt in seinem Buch „Wem gehört die Zukunft?“ [7] ein Modell vor, das Anwender an Einnahmen, die basierend auf deren Daten erzielt werden, beteiligt – eine, eine Idee deren Umsetzung nicht einfach werden dürfte.

Grundsätzlich ist das Bezahlen von Diensten mit persönlichen Daten ein legitimes Geschäftsmodell. Dabei ist die monetäre Bewertung persönlicher Daten ein komplexes Thema. Insbesondere ist die Bewertung asynchron, d. h. der Wert der Daten für eine Organisation, die diese verarbeitet, wird ein völlig anderer sein, als der Wert aus Sicht des Einzelnen, der diese Daten zur Verfügung stellt. Die Financial Times hat eine Reihe von Unternehmen in den USA befragt, die in großem Stil mit persönlichen Daten handeln. Basierend darauf wurde ein Kalkulator erstellt, mit dem sich der Wert eines Datensatzes zu einer Person in Abhängigkeit von den enthaltenen Merkmalen berechnen lässt[11]. Für den Einzelnen gibt es einen solchen vermeintlich klar festzulegenden Wert seiner persönlichen Informationen nicht, dieser hängt von der persönlichen Bewertung und dem Kontext ab.

74.4.1 Praktische Umsetzung von Datenschutz in mobilen Diensten

Ein Anbieter von Dienstleistungen sollte vor dem Hintergrund dieser Überlegungen eine klare Strategie festlegen, wie mit dem Thema Datenschutz umgegangen wird. Dazu gibt es Stand heute wenig konkrete Handlungsempfehlungen. Einen Vorschlag liefert das von Cavoukian [3] entwickelte Privacy by Design Konzept, das sieben Grundprinzipien formuliert, die bei der Entwicklung von Anwendungen berücksichtigt werden sollten. Ein umfassendes theoretisches Rahmenwerk bietet das Privacy Security Trust (PST) Framework von Morton et al. [8]. Im Folgenden werden die wesentlichen Themen beleuchtet, die sich aus diesen Konzepten für das Design von mobilen Diensten in der Praxis ergeben.

[10] http://www.flurry.com/bid/99013/The-History-of-App-Pricing-And-Why-Most-Apps-Are-Free#.VCvo7il_sVW (Letzter Aufruf: 1.10.2014).

[11] http://www.ft.com/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html (Letzter Aufruf: 1.10.2014).

74.4.2 Datenschutzprinzipien

Inwieweit Anwender ihre Daten Organisationen bereitstellen, hängt insbesondere mit Vertrauen zusammen. D. h. zunächst sollte eine grundsätzliche Strategie im Unternehmen festgelegt werden, wie mit Daten der Nutzer umgegangen wird. Zumindest müssen rechtliche Bestimmungen des Datenschutzes erfüllt werden. Eines der Grundprinzipien ist dabei die Datensparsamkeit und Datenvermeidung, d. h. es sollten nur so viel Daten erhoben werden, wie unbedingt nötig (Bundesdatenschutzgesetz, § 3a), was sehr weit von der derzeitigen Datensammelpraxis einer Vielzahl mobiler Apps entfernt ist.

Wie diese Anforderungen in der Praxis umgesetzt werden, also ob diese nur formal erfüllt werden oder darüber hinaus gehende Prinzipien festgelegt werden, hängt vom Geschäftsmodell des Unternehmens ab. Diese Prinzipien bilden aber die Grundlage und allgemeine Handlungsorientierung für weitere Dienste.

74.4.3 Verarbeitung von Informationen

Für den konkreten Dienst sollte ein Konzept erstellt werden, welche Informationen erhoben werden und zu welchem Zweck: Wie werden diese gesammelt, auf welche Art und Weise wo gespeichert, wie verarbeitet und dabei möglicherweise mit anderen Informationen verknüpft, sowie wann werden diese letztlich wieder gelöscht. An wen werden die Informationen weitergegeben, wer hat intern Zugriff auf diese Informationen. Letztlich eine klare Beschreibung des Lebenszyklus der Informationen eines Anwenders innerhalb eines Dienstes, als Basis für dessen technische Umsetzung.

74.4.4 Transparenz

Abhängig vom Geschäftsmodell muss ein Unternehmen entscheiden, wie viel Transparenz es gegenüber seinen Anwendern beim Umgang mit persönlichen Daten will. Für das Beispiel der Flashlight App, deren Ziel es ist, Benutzerdaten zu sammeln, diese an Analysefirmen zu verkaufen, wo diese mit Hilfe von Big Data Technologien mit anderen Informationen kombiniert werden, ist Transparenz gegenüber dem Benutzer keine Option. Das Geschäftsmodell besteht letztlich im versteckten Sammeln von Daten. Andererseits sind Anwender durchaus bereit Informationen zu teilen, wenn es im passenden Kontext stattfindet und dieser klar ersichtlich ist [5]. So kann man sich für die Nutzung der Kartenapp von Apple entscheiden, die permanent Information zu Standort und Bewegung an Apple meldet. Auf Basis dieser Daten und den Daten tausender anderer Nutzer wird jederzeit ein aktuelles Bild der Verkehrssituation erzeugt, d. h. der Anwender gibt Daten von sich preis, erhält dafür aber einen Mehrwert.

Apple weist den Anwender auf die Erhebung dieser Daten in einem ca. 30 seitigen, sogenannten End User License Agreement (EULA) hin, dem dieser, will er das Gerät nutzen, zustimmen muss und damit eine Freigabe für diese Nutzung erteilt.

Ein EULA ist aber kein geeignetes Mittel, um Transparenz zu schaffen. Laut einer Studie von Böhme und Köpsell [1] stimmen mehr als 50 % der Nutzer diesem in weniger als 8 Sekunden – also weitestgehend ungelesen – zu. Darüber hinaus kommt die Studie zu dem Ergebnis, dass Anwender Regelungen umso eher unreflektiert zustimmen, je mehr diese einem EULA entsprechen und damit je komplexer diese sind.

Dem steht der Ansatz entgegen, von Anwendern die Zustimmung zur Nutzung bestimmter Daten kontextbezogen einzuholen. Im Beispiel Kartenapp würde dies bedeuten den Benutzer bei einer erstmaligen Nutzung darauf hinzuweisen, welche Daten zu welchem Zweck gesammelt werden und zu fragen, ob dieser damit einverstanden ist.

74.4.5 Benutzererfahrung

Anwender wollen eine bestimmte Funktionalität intuitiv benutzen und Sicherheit und Benutzerfreundlichkeit sind dabei oft komplementäre Ziele. Je stärker ein Passwort ist, desto umständlicher wird die Benutzung eines Dienstes. Dementsprechend gelten sichere Lösungen häufig als schwer bedienbar, was dazu führt, dass Anwender Mittel und Wege finden, diese Mechanismen zu umgehen.

Wie auch beim Thema Datensicherheit wird eine Umsetzung von Maßnahmen zum Datenschutz nur dann erfolgreich sein, wenn sich der Dienst einfach und intuitiv bedienen lässt und damit eine hohe Benutzerfreundlichkeit gegeben ist. Das gelingt am besten, wenn Datensicherheit und Datenschutz von Anfang inhärenter Teil des Designprozesses mobiler Dienste und Lösungen sind. Werden diese nachträglich, um solche Funktionalität ergänzt, möglicherweise erst nachdem datenschutzrelevante Vorfälle öffentlich wurden, ist es deutlich schwieriger eine durchgängige Benutzererfahrung zu gewährleisten [3].

74.5 Ausblick

Basierend auf den neuen technischen Möglichkeiten mobiler Endgeräte ergibt sich einerseits eine Vielzahl neuer Geschäftsmodelle. Andererseits erlauben diese drastische Eingriffe in die Privatsphäre des Einzelnen, mit möglichweise erheblichen persönlichen Auswirkungen, eine Erkenntnis für die gerade erst langsam ein allgemeines Bewusstsein entsteht.

Galten Datenschutz und Datensicherheit in der Vergangenheit als Nischenthemen, entdecken Anbieter von mobilen Diensten das Thema gerade als Möglichkeit sich am Markt zu differenzieren[12], sicherlich nicht zuletzt aufgrund der starken öffentlichen Wahrnehmung in Folge der NSA-Affäre.

[12] http://www.macworld.com/article/2685600/apple-updates-privacy-policy-we-sell-great-products-not-your-data-says-tim-cook.html (Letzter Aufruf: 1.10.2014).

Die Themen Datensicherheit und Datenschutz sollten nicht den Kryptologen und den Rechtsabteilungen überlassen werden, sonst führt dies zu Lösungen, die von Anwendern nicht genutzt und zu Vereinbarungen, die von diesen nicht verstanden werden. Bei Datensicherheit und Datenschutz sollte der Anwender im Mittelpunkt stehen.

Literatur

1. Böhme, R., & Köpsell, S. (2010). Trained to accept? A field experiment on consent dialogs. In *Human Factors in Computing Systems (CHI)*.
2. Bundesamt für Sicherheit in der Informationstechnik. (2006). Mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdungen und Schutzmaßnahmen.
3. Cavoukian, A. (2011). Privacy by design: The 7 foundational principles.
4. Heider, J., & El Khayari, E. (2012). iOS keychain weakness FAQ. Frauenhofer Institute for Secure Information Technology (SIT).
5. Krasnova, H., Gunther, O., Spiekermann, S., & Koroleva, K. (2009). Privacy concerns and identity in online social networks. *Identity in the Information Society 2*(1)*,* 39-63.
6. Kumaraguru, P., & Cranor, L. F. (2005). Privacy indexes: A survey of Westin's studies. *ISRI Technical Report*.
7. Lanier, J. (2014). Wem gehört die Zukunft? Du bist nicht der Kunde der Internetkonzerne. Du bist ihr Produkt.
8. Morton, A., & Sasse, M. A. (2012). Privacy is a process, not a PET: A theory for effective privacy practice. In *Workshop on New Security Paradigms*.
9. Schneier, B. (2004). Secrets and lies: Digital security in a networked world.
10. Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H., & Borgthorsson, H. (2014). Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. In *Human Factors in Computing Systems* (CHI).
11. Woodruff, A., Pihur, V., Consolvo, S., Schmidt, L., Brandimarte, L., & Acquisti, A. (2014). Would a privacy fundamentalist sell their DNA for $ 1000… if nothing bad happened as a result? The Westin categories, behavioral intentions, and consequences. In *Usable Privacy and Security (SOUPS)*.
12. von Zezschwitz, E., Koslow, A., De Luca, A., & Hussman, H. (2013). Making graphic-based authentication secure against smudge attacks. In *Intelligent user interfaces (IUI)*.