Eric Bodden, Siegfried Rasthofer, Philipp Richter, Alexander Roßnagel

Schutzmaßnahmen gegen datenschutzunfreundliche Smartphone-Apps

Technische Möglichkeiten und rechtliche Zulässigkeit des Selbstdatenschutzes bei Apps

Privacy Enhancing Technologies, die den Umgang von Smartphone-Apps mit personenbezogenen Daten überwachen und unerwünschte Übermittlungen verhindern, können mit dem Urheberrecht in Konflikt geraden. Der Beitrag untersucht die technischen Möglichkeiten des Selbstdatenschutzes und nimmt eine erste rechtliche Bewertung vor.*

Prof. Dr. Eric Bodden

Kooperationsprofessor für Secure Software Engineering am Fraunhofer SIT und an der TU Darmstadt.

E-Mail: eric.bodden@ec-spride.de

Siegfried Rasthofer

Wissenschaftlicher Mitarbeiter in der Forschungsgruppe Secure Software Engineering an der TU Darmstadt.

E-Mail: siegfried.rasthofer@cased.de

Dr. Philipp Richter

Institut für Wirtschaftsrecht, Universität Kassel. Fachgebiet Öffentliches Recht, insb. Umwelt- und Technikrecht. Projektgruppe verfassungsverträgliche Technikgestaltung (provet).
E-Mail: prichter@uni-kassel.de

Prof. Dr. Alexander Roßnagel

Wiss. Leiter der „Projektgruppe verfassungsverträgliche Technikgestaltung" (provet) und Direktor des Forschungszentrums für Informationstechnik-Gestaltung (ITeg) an der Universität Kassel.
E-Mail: a.rossnagel@uni-kassel.de

1 Unsichere und böswillige Apps

App-Stores wie z. B. Googles hauseigener „Play Store" bieten unterschiedliche Arten von Apps für den Download an. Ein Nutzer wählt sich eine App aus und kann diese mit nur wenigen Klicks herunterladen und installieren. Die hohe Beliebtheit von Smartphones ist zum größten Teil auf die Vielfalt der Apps in den Stores und das einfache Prinzip der Installation zurückzuführen. Es gibt für fast alle Vorlieben der Nutzer Apps im App-Store, wie z. B. Nachrichtenprogramme, Musik-Player, Spiele, Online-Banking oder Social Media.

Trotz der generellen Vorteile von Apps gibt es leider auch viele Exemplare, die unsicher oder gar böswillig sind. Derzeit findet sich in den großen App-Stores eine Vielzahl von Apps, die personenbezogene Daten wie z. B. Standortdaten oder Inhalte des Adressbuchs an Dritte schicken.[1]

Dies wird zum einen durch Werbeplugins in Apps verursacht. Diese Werbeplugins werden explizit vom Entwickler in die entwickelte App integriert. Dies ist dadurch zu begründen, dass Entwickler ihre Apps zum größten Teil kostenlos anbieten und durch die integrierte Werbung von Werbeanbietern Geld einnehmen. Diese Plugins wiederum versuchen möglichst gute Profile der Nutzer zu bilden, indem sie personenbezogene Daten verwenden, um gezielte, auf den Nutzer zugeschnittene Werbung anzuzeigen. Ein Beispiel hierfür ist das Übertragen von Standortdaten, die dazu verwendet werden, um Werbung für Anbieter aus der direkten Umgebung einzublenden. Dieses Problem ist allgegenwärtig in unterschiedlichen Apps. Ein prominentes Beispiel hierfür ist Ingress[2], ein Augmented-Reality-Spiel von Google.

* Der Text ist aus der Kooperation im Center for Advanced Security Darmstadt (CASED) hervorgegangen. CASED wird von der Landes-Offensive zur Entwicklung wissenschaftlich-ökonomischer Exzellenz (LOEWE) des Landes Hessen von 2008 bis 2014 gefördert.

1 *Venne/Elkenberg/Schmidt*, Selbstbedienungsladen Smartphone, c't 7/12, 114, http://www.heise.de/ct/artikel/Selbstbedienungsladen-Smartphone-1464717.html; test.de, Datenschutz bei Apps: Welche Apps Ihre Daten ausspähen; http://www.test.de/Datenschutz-bei-Apps-Welche-Apps-Ihre-Daten-ausspaehen-4378643-0/.

2 http://www.heise.de/newsticker/meldung/Googles-GPS-Spiel-Ingress-Werbung-an-virtuellen-Spielorten-1930296.html.

Zum anderen gibt es viele böswillige Apps, die versuchen dem Nutzer insbesondere finanziellen Schaden zuzufügen, um daraus Profit zu schlagen. Ein Beispiel hierfür wäre der Versand von überteuerten SMS oder die Initiierung von Telefonanrufen an überteuerte Premium-Nummern. Solche Art von Apps sind für den Nutzer nicht oder nur schwer zu bemerken.

Noch nicht sehr verbreitet, aber dennoch vorhanden, sind bösartige Applikationen, wie sie aus der PC-Welt bekannt sind. Sie versuchen die Kontrolle über das Gerät zu gewinnen. Diese Apps nutzen Schwachstellen auf dem Smartphone aus, um dann die höchsten Rechte auf dem Gerät zu erlangen (root). Anschließend kann ein Angreifer Aktivitäten im Namen des Smartphone-Nutzers ausüben, wie z. B. Anrufe tätigen oder SMS versenden.

2 Abwehrmöglichkeiten

Am Beispiel von Android Apps wird im Folgenden untersucht, welche technischen Möglichkeiten der Nutzer hat, um sein Smartphone gegen solche Angriffe zu schützen. Hierbei sind Maßnahmen, die direkt in die Software der App eingreifen und diese verändern, von solchen Maßnahmen zu unterscheiden, die zwar in das Betriebssystem des Smartphones eingreifen, jedoch nicht in die Software der Apps.

2.1 Veränderung der Software

Konkret geht es darum, Endbenutzern die Möglichkeit zu geben, Apps im speziellen oder Softwareprogramme im allgemeinen bei der Installation auf einem System (hier: Mobiltelefon) so zu verändern, dass dabei bestimmte Sicherheitsgarantien etabliert werden können. So könnten z. B. ungewollte Programmteile einfach entfernt werden, oder aber eine Sicherheitssoftware könnte Apps bei der Installation auf dem Handy automatisch um Sicherheitschecks erweitern, indem die Software den Programmcode der App ergänzt. Als Resultat bekommt der Nutzer hierdurch eine veränderte App installiert, deren Ausführung durch hinzugefügten Programmcode überwacht und beeinflusst wird.

Zum Beispiel könnten Standortdaten so vergröbert werden, dass der Nutzer anhand dieser Daten nicht mehr exakt geortet werden kann. Oder aber der Programmcode erkennt, dass eine App private Daten versenden möchte, und informiert den Nutzer hierüber, der das Senden unterbinden oder die Daten verändern kann.

2.2 Veränderung des Betriebssystems

Eine Alternative zur Veränderung des App-Codes bildet die Veränderung des Betriebssystems. Dabei bleibt der Programmcode der Apps unverändert; statt dessen wird das Betriebssystem selbst um Code angereichert, der beispielsweise die Handhabung privater Daten durch Apps bei deren Ausführung überwacht. Um das veränderte Betriebssystem nutzen zu können, sind einige technische Schritte von Nöten bis es vom Nutzer genutzt werden.

2.3 Technische Vor- und Nachteile

Die Veränderung des Betriebssystems ist technisch möglich, erfordert aber in der Regel die aktive Unterstützung der Hersteller. Google beispielsweise hat Android mit einfachen Sicherheitskontrollen erweitert, diese erweisen sich aber teilweise als wenig geeignet für die Praxis:

- So gibt es in Android 4.2 eine Funktion, die Benutzer warnt, wenn Apps mit schädlichem Verhalten installiert werden.[3] Allerdings werden nur wenige Schad-Apps vom Betriebssystem erkannt.[4]
- Ebenfalls in Android 4.2 gibt es einen Sicherheitsmechanismus, der den Nutzer im Falle eines ungewollten Sendens von überteuerten SMS warnt. Dieser Mechanismus hat sich als wirkungsvoll erwiesen, leider gibt es für die Initiirung von überteuerten Telefonanrufen noch keinen Sicherheitsmechanismus.
- In Android 4.3 gibt es eine versteckte Funktion, mit der der Zugriff von Apps auf Ressourcen reguliert werden kann. So lässt sich beispielsweise für bestimmte Apps der Zugriff auf Standortdaten ein oder ausschalten. Diese Funktion befindet sich noch im Beta-Stadium und bietet dem Benutzer auch keine Möglichkeit, feingranulare Einstellungen zu tätigen: entweder wird der Zugriff auf Ressourcen komplett verhindert oder gar nicht.

Erweiterungen um Sicherheitskontrollen im Betriebssystem, wie beispielsweise Warnungen über das Versenden von persönlichen Daten, sind in der Regel von Google nicht zu erwarten. Dies ist dadurch zu begründen, dass diese Art von Kontrollen die Ausführung von Apps verlangsamen können. Sollte ein Nutzer dennoch diese Art von Kontrollen wünschen, kann er auf bereits veränderte Android-basierende Betriebssysteme, wie beispielsweise TaintDroid[5], zurückgreifen. Die Installation des neuen Betriebssystems auf dem Mobilgerät erweist sich jedoch als zu kompliziert, was ohne technisches Wissen gar unmöglich ist.

Die Absicherung der Ausführung einer App durch das Umschreiben des Programmcodes ist für den Nutzer höchst komfortabel, da er hierzu das auf dem Telefon befindlichen Betriebssystems nicht ändern muss. Technische Nachteile bestehen lediglich darin, dass die eingebauten Sicherheitsüberprüfungen die Ausführung der App gegebenenfalls verlangsamen oder in Teilen behindern können, da die App nicht im Hinblick auf eine solche Technologie entworfen wurde.

3 Urheberrechtliche Bewertung

Rechtlich stellt sich in diesem Zusammenhang vor allem die Frage der urheberrechtlichen Zulässigkeit: Wären Code-Modifikationen an Apps oder dem Betriebssystem nach aktueller Rechtslage überhaupt erlaubt? Soweit diese Frage zu verneinen wäre, würde sich die Frage anschließen, ob und wie die aktuelle Rechtslage angepasst werden müsste, um den Einsatz solcher Software zu ermöglichen und dadurch Rechtssicherheit zu schaffen für Anbieter und Nutzer von Apps einerseits und für die Anbieter von App-bezogenen Sicherheitswerkzeugen andererseits.

Bei der urheberrechtlichen Bewertung ist zu unterscheiden zwischen der Methode, den Code der App zu verändern, und der Methode, das Betriebssystem des eigenen Geräts zu verändern, ohne in den Code der App einzugreifen. Zu differenzieren ist auch, ob die App als Closed Source oder als Open Source vertrieben wird.

3 http://developer.android.com/about/versions/jelly-bean.html
4 http://www.cs.ncsu.edu/faculty/jiang/appverify/
5 http://www.appanalysis.org

3.1 Zulässigkeit von Codemanipulationen

Die §§ 69a ff. UrhG (Besondere Bestimmungen für Computerprogramme) setzen die europäische Richtlinie 91/250/EWG über den Rechtsschutz von Computerprogrammen um. Gemäß § 69a UrhG werden als Computerprogramme Programme jeder Gestalt, einschließlich des Entwurfmaterials geschützt. Der Begriff ist weit zu verstehen. Er umfasst Betriebssysteme, Anwendungen, Browser, Suchmaschinen und viele weitere Befehlsfolgen, die bewirken, dass eine informationsverarbeitende Maschine eine bestimmte Funktion ausführt.[6] Die hier betrachteten Android-Apps, inklusive solcher Programmteile, die Nutzerdaten erheben und speichern, stellen Computerprogramme in diesem Sinne dar.

Nach § 69c Nr. 2 UrhG hat der Rechteinhaber das ausschließliche Recht, die Bearbeitung, das Arrangement und andere Umarbeitungen vorzunehmen. Es handelt sich um ein umfassendes Recht, das alle Abänderungen, insbesondere solche des Programmcodes, inklusive der Fehlerberichtigung einschließt. Bei einer Fehlerkorrektur, die nicht mehr als 5 % des Programmcodes betrifft, wurde stattdessen eine Vervielfältigung angenommen,[7] die aber nach § 69c Nr. 1 UrhG ebenfalls nur dem Rechteinhaber zusteht. Rechteinhaber ist dabei nicht der Käufer des Programms, sondern sein Urheber.[8] Änderungen des Funktionsumfangs, wie hier die Entfernung von Programmteilen, die personenbezogene Daten erheben, oder das Hinzufügen von Programmteilen, die solches überwachen und verhindern, fallen grundsätzlich unter dieses Bearbeitungsrecht.[9]

Eine freie Benutzung gemäß § 24 Abs. 1 UrhG läge nicht vor. Hierzu wäre es notwendig, angeregt durch das ursprüngliche Werk ein selbständiges eigenes Werk zu schaffen, bei dem die Züge des älteren Werks verblassen.[10] Im vorliegenden Fall würden aber nur einzelne Elemente der App, wie der unerwünschte Zugriff auf personenbezogene Daten, entfernt oder verändert. Die zentralen Funktionen der Anwendung wären weiterhin vorhanden. Die Nutzer möchten ja gerade die ursprüngliche App nutzen, nur ohne die unerwünschten „Nebenwirkungen".

Die Veränderung eines Softwareprogramms durch Streichung unerwünschter, Daten erhebender Befehle ist somit ohne die Einwilligung des Rechteinhabers urheberrechtlich grundsätzlich unzulässig.

Die Veränderung von Programmabläufen ist allerdings auch möglich, ohne tatsächlich den Code des auf der Festplatte gespeicherten Programms an sich zu verändern. Schutzprogramme könnten den Programmcode auch während der Ausführung im Arbeitsspeicher verändern. Obwohl die Kopie des Programms auf der Festplatte dabei in seiner Substanz integer bliebe und nur der Programmablauf manipuliert würde, wird auch dies als Umarbeitung im Sinne von § 69c Nr. 2 UrhG eingeordnet. Begründet wird dies damit, dass es nicht von den technischen Möglichkeiten zur Programmveränderung abhängen könne, ob der Schutz des Urheberrechts greife oder nicht.[11]

Nach dieser weiten Auslegung dürften auch andere technische Möglichkeiten, auf den Programmablauf einzuwirken, als Bearbeitung einzustufen sein. Nutzer, die solche Veränderungen vornehmen, um Datenschutz zu betreiben, würden sich Unterlassungs- und möglicherweise Schadensersatzansprüchen gemäß § 97 UrhG sowie Ansprüchen auf Vernichtung des veränderten Programms gemäß §§ 69f und 98 UrhG aussetzen.

Der Vertrieb von Programmen, die diese Veränderungen ermöglichen, wäre zwar nicht selbst gemäß § 95a Abs. 3 UrhG unzulässig, da § 69a Abs. 5 UrhG dessen Anwendbarkeit für (reine) Computerprogramme ausschließt.[12] Er würde aber im Fall der Bearbeitung durch den Nutzer wohl zu Unterlassungs- und eventuell Schadensersatzansprüchen gegen den Vertreiber wegen Teilnahme[13] aus § 97 UrhG führen.

3.2 Open Source Code

Wird eine App allerdings unter einer Open Source-Lizenz angeboten[14], kann sich die Bewertung ändern. Solche Lizenzen ermöglichen in der Regel die freie Bearbeitung eines Computerprogramms. Zum Beispiel enthält Art. 5 der GNU General Public License[15] das Recht, Veränderungen oder die nötigen Mittel zur Veränderung von Programmen zu verbreiten, soweit die dortigen Voraussetzungen erfüllt werden, wie zum Beispiel die Verbreitung der Veränderungen unter der gleichen Lizenz und die Kennzeichnung als Bearbeitung.

3.3 Zulässigkeit von Berechtigungsentziehungen ohne Veränderung des Codes

Neben der Veränderung des App-Codes in der Substanz oder im Arbeitsspeicher besteht auch die Möglichkeit, das Betriebssystem des Endgeräts so zu verändern oder durch ein Programm verändern zu lassen, dass die unter 3.1 aufgezeigten Ergebnisse auf Betriebsystemebene ausgeführt werden. Die Veränderung des Betriebssystems ist im Fall von Android urheberrechtlich grundsätzlich möglich, da es sich weitgehend um Open-Source-Software unter einer Apache-Lizenz[16] handelt, die Modifikationen zulässt. Der Systemkern ist unter der GNU General Public License Version 2 veröffentlicht.

Durch das veränderte Betriebssystem können vergleichbare Ergebnisse erzielt werden wie bei Veränderung des Programmcodes. Das kann auf unterschiedlichem Wege erfolgen:

- Zum einen kann das Betriebssystem einfach Warnungen an den Nutzer abgeben, dass die App gerade bestimmte Daten erhebt. Für den Nutzer kann sich hieraus die Konsequenz ergeben, dass er die App deaktiviert oder deinstalliert.

In diesem Fall würde weder in den Code der App noch in ihren Ablauf eingegriffen, daher ist diese Variante urheberrechtlich unbedenklich.

- Oder aber das veränderte Betriebssystem kann dafür sorgen, dass der Ablauf der App verändert wird. Zwar wird nicht der Code der App selbst manipuliert, weder direkt auf der Festplatte noch bei der Ausführung im Arbeitsspeicher. Vielmehr wird

6 *Dreier*, in: *Dreier/Schulze*, UrhG, 4. Aufl. München 2013, § 69a UrhG, Rn. 12.
7 *BGH*, NJW-RR 1990, 361 (362).
8 *Dreier* (Fn. 6), § 69c UrhG, Rn. 2, Rn. 15.
9 *Wiebe*, in: *Spindler/Schuster*, Recht der elektronischen Medien, 2. Aufl. München 2011, § 69c UrhG, Rn. 9.
10 *BGH* ,GRUR 1994, 191 (193).
11 *OLG Hamburg*, GRUR-RR 2013, 13 (14 f.).
12 Auf Computerspiele wird die Norm hingegen angewendet, da diese nicht bloß als Programme, sondern auch als Film- und Tonwerke eingeordnet werden, *LG München* I MMR 2008, 839; a.A. *Schröder*, Rechtmäßigkeit von Modchips, MMR 2013, 80.
13 S. *LG München* I MMR 2008, 839; *OLG Hamburg*, GRUR-RR 2013, 13 (16).
14 Eine Liste von Open Source Anwendungen für Android findet sich unter: http://www.aopensource.com/.
15 Version 3, 29.6.2007.
16 http://www.apache.org/licenses/LICENSE-2.0.html.

die Interpretation des Programms durch eine virtuelle Maschine verändert. Der Code bleibt intakt, wird aber anders verarbeitet: zum Beispiel könnte ein Programmbefehl „Sende die folgenden Daten an den folgenden Server" vom Betriebssystem einfach ignoriert werden.

Letztendlich kommt es hierdurch auch in diesem Fall dazu, dass der Ablauf der App nicht so stattfindet, wie vom Urheber beabsichtigt, denn sie wurde für das unveränderte Betriebssystem entwickelt. Wird die weite Auslegung des Bearbeitungsbegriffs des OLG Hamburg, die stärker auf die korrekte Ausführung des Programms als auf die technischen Einzelheiten abstellt,[17] bestätigt und weiter verfolgt, ist es nicht auszuschließen, dass auch die im Hinblick auf die App getätigten Veränderungen des Betriebssystems als Umarbeitung der App eingestuft würden.

3.4 Zwischenergebnis

Bei einer reinen Betrachtung nach Urheberrecht wäre die erste Alternative (Änderung des Codes der App) unzulässig und die zweite (Änderung des Betriebssystems) unter bestimmten Bedingungen ebenfalls. Dies erscheint jedoch unbefriedigend, wenn dadurch Funktionen einer App geschützt werden, die illegale Aktionen ermöglichen. Zu prüfen ist daher, ob der Einbezug weiterer Rechtsaspekte nicht zu einem anderen Ergebnis führen müsste.

4 Abwehr unzulässiger App-Aktivitäten

4.1 Datenschutzrechtliche Bewertung

Viele der von Apps verarbeiteten Daten können einen Personenbezug im Sinne des § 3 Abs. 1 BDSG aufweisen. So können Apps eine namentliche Registrierung verlangen. Aber auch ohne Registrierung enthalten insbesondere Smartphones und Tablets viele Daten, mit denen die Nutzer und weitere Personen identifiziert werden können: Telefonbücher enthalten ebenso Namens- und Adressinformationen wie Inhalte von SMS-Nachrichten und die mit der App selbst vom Nutzer verarbeiteten Inhalte, letzteres insbesondere bei Messaging-Diensten und Sozialen Netzwerken. In Verbindung mit solchen Informationen können auch Standortdaten des Endgeräts und eigentlich „anonym" durchgeführte Aktivitäten den Nutzern namentlich zugeordnet werden.[18]

Die Sammlung und Übermittlung personenbezogener Daten ist jedoch ein Eingriff in das Recht auf informationelle Selbstbestimmung. Dieser Eingriff ist nur dann gerechtfertigt, wenn er durch eine datenschutzrechtliche Einwilligung oder eine Rechtsregelung gerechtfertigt ist, die den Zweck der Datenverarbeitung genau bestimmt.

4.2 Datenschutzrechtliche Einwilligung

Der Download einer App ist ein Telemediendienst,[19] daher gelten für eine datenschutzrechtliche Einwilligung nicht die Anforderungen der Schriftform nach § 4a Abs. 1 BDSG, sondern der elektronischen Einwilligung nach § 13 Abs. 2 TMG.[20] Voraussetzung einer wirksamen elektronischen Einwilligung nach § 13 Abs. 2 TMG ist nach Nr. 1 zunächst eine bewusste und eindeutige Erteilung durch den Nutzer durch aktives Tun.[21] Dies soll bei App-Downloads dadurch erreicht werden, dass die Nutzer bei der Installation bestätigen müssen, mit verschiedenen Zugriffen auf Daten auf ihrem Endgerät einverstanden zu sein.

Allerdings sind hierbei die Erläuterungen der beabsichtigten Datenverarbeitungen in der Regel sehr abstrakt gehalten. Sie erschöpfen sich meist in der Angabe, die App werde auf bestimmte Datensätze (z. B. Anrufe, Standortdaten) zugreifen. Zu welchem Zweck diese Erhebung erfolgt, was mit den Daten dann geschieht, wer sie erhält und ob und wann sie gelöscht werden, ist beim „Akzeptieren" dieser „Berechtigungen" nicht zu erkennen. Dies ist für eine wirksame Einwilligung aber notwendig.[22]

Im Download-Fenster vieler (keineswegs aller) Apps findet sich ein Link auf eine Datenschutzerklärung. Dieser Link ist von Endgerät zu Endgerät unterschiedlich leicht aufzufinden. Zum Beispiel ist er auf Tablet-Computern in einer Seitenleiste angeordnet und durch kurzes Herunterscrollen zu sehen. Auf Smartphones hingegen fehlt die seitliche Leiste und Nutzer müssen weit nach unten scrollen. Erst unter den Nutzerkommentaren zur App und Vorschlägen für weitere Apps findet sich am Ende der Seite die Datenschutzerklärung.

Werden Umfang und Zweck des beabsichtigten Datenumgangs aus der Datenschutzerklärung für die Betroffenen klar erkennbar, könnten diese Informationen das „Akzeptieren" der Berechtigungen doch zu einer wirksamen Einwilligung werden lassen. Es wird hier im Einzelfall darauf ankommen, ob die Datenschutzerklärung im Zusammenhang mit dem „Akzeptieren" wahrgenommen werden kann. Da sich im „Akzeptieren"-Fenster in der Regel kein Hinweis oder Link auf sie findet, hängt dies von ihrer örtlichen Platzierung auf der Download-Seite ab und kann je nach Anzeige auf dem Endgerät sehr zweifelhaft sein. Ist die Einwilligungserklärung in der Datenschutzerklärung enthalten, könnte sie durch das „Akzeptieren" der Berechtigungen bestätigt werden. Soweit jedoch das „Akzeptieren"-Fenster keinen Hinweis auf die Datenschutzerklärung enthält und diese erst durch Scrollen überhaupt wahrnehmbar ist, wird eine eindeutige Einwilligung in der Datenschutzerklärung durch „Akzeptieren" der App-Berechtigungen nur in seltenen Fällen anzunehmen sein.

Eine Einwilligung könnte auch in Allgemeinen Geschäftsbedingungen (AGB) enthalten sein. In der Regel finden sich beim Download von Android-Apps keine AGB. Liegen aber AGB vor, die eine datenschutzrechtliche Einwilligung enthalten, wären diese gemäß § 4a Abs. 1 Satz 4 BDSG, der auch für elektronisch abgegebene Einwilligungen gilt, gegenüber den übrigen Erklärungen deutlich hervorzuheben. Auf solche Erklärungen wäre gesondert hinzuweisen und sie müssten entsprechend markiert werden, so dass Nutzer klar erkennen, dass sie zur Einwilligung in den Umgang mit personenbezogenen Daten aufgefordert werden. Die ‚drucktechnische' Gestaltung müsste die Aufmerksamkeit der Betroffenen gezielt auf die Einwilligungserklärung lenken.[23]

Gemäß § 13 Abs. 2 Nr. 3 TMG müssen die Nutzer den Inhalt der Einwilligung jederzeit abrufen können. Die oben beschriebenen Berechtigungen und Datenschutzerklärungen können in „Google Play", der Bezugsplattform für Android Apps, immer wieder aufgerufen werden. Sie stellen aber keine abrufbare Ein-

17 *OLG Hamburg*, GRUR-RR 2013, 13 (14 f.).
18 S. hierzu auch: *Sachs/*Meder, ZD 2013, 303 (304).
19 *Sachs/Meder* (Fn. 18).
20 S. hierzu *Jandt/Schaar/Schulz*, in: Roßnagel (Hrsg.), Recht der Telemediendienste, München 2013, § 13 TMG, Rn. 66.
21 *Jandt/Schaar/Schulz* (Fn. 20), § 13 TMG, Rn. 73.
22 *Simitis*, in: *Simitis*, BDSG, 7. Aufl., Baden-Baden 2011, § 4a BDSG, Rn. 70 ff.
23 *Simitis* (Fn. 22), § 4a BDSG, Rn. 40 f.

willigung in diesem Sinne dar. Die Einwilligung enthält vielmehr auch die Erklärung des Nutzers, hiermit einverstanden zu sein und ist deshalb ein personenbezogenes Datum.[24] Überdies kann die Datenschutzerklärung sich ändern und muss daher nicht den gleichen Inhalt wie zum Zeitpunkt der Installation aufweisen. Sie kommt auch aus diesem Grund nicht als Abruf einer Einwilligung in Betracht.

Nach Nr. 4 müssen die Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen können. Hierzu reicht die Deinstallation der App, die ein weiteres Erheben von Daten verhindert, nicht aus, da sich der Widerruf auch auf den weiteren Umgang mit bereits erhobenen Daten beziehen können muss. Die Anbieter müssen daher technische Möglichkeiten bereithalten, mit denen die Nutzer den Widerruf ausführen können,[25] wie z. B. eine Schaltfläche oder zumindest einen E-Mail-Kontakt. Bei Android-Apps ist in der Regel in „Google-Play" die E-Mail-Adresse des Entwicklers der App neben der Datenschutzerklärung angegeben.

Der Widerruf kann auch konkludent erfolgen, wenn er ausreichend eindeutig ist.[26] Der Einsatz einer veränderten Version der App, die die Erhebung personenbezogener Daten verhindert, ließe an Deutlichkeit eigentlich nichts zu wünschen übrig und könnte daher als Widerrufsmöglichkeit in Frage kommen. Hierzu müsste dem App-Anbieter aber erkennbar sein, dass ein bestimmter Nutzer etwas an der App verändert hat und was.

Dies wäre relativ aufwendig und würde ein Aktivwerden des Anbieters erfordern. Die veränderten Apps haben von der Original-Version abweichende Programm-Signaturen, die als Einweg-Hashsummen aus den Programmteilen gebildet werden. Der Anbieter merkt aber nicht automatisch, dass eine veränderte App von einem bestimmten Nutzer eingesetzt wird und was verändert wurde. Dass veränderte Versionen seiner App im Umlauf sind, müsste er also zunächst erfahren. Er könnte sich dann ebenfalls eine veränderte Version besorgen, die Veränderungen auf Maschinencode-Ebene untersuchen und hierdurch erfahren, welche Signatur für welche Veränderungen steht. Um das Nutzen der veränderten Signatur dann als Widerruf eines bestimmten Nutzers zu deuten, müsste er überdies noch herausfinden, welche Nutzer die App mit dieser Signatur installiert haben. Diesen Aufwand wird er im Hinblick auf den Widerruf der Einwilligung kaum betreiben, da er selbst hieran kein Interesse haben wird. Als Widerrufsmöglichkeit kommt das Verändern der App daher theoretisch, nicht aber in der Praxis in Frage.

In § 28 Abs. 3b BDSG ist für Datenverarbeitung zum Zweck der Werbung ein Kopplungsverbot vorgesehen. Die Verarbeitung personenbezogener Daten zu Werbezwecken kann nicht auf eine Einwilligung der Betroffenen gestützt werden, wenn der Abschluss des Vertrags hiervon abhängt und den Betroffenen ein anderer Zugang zu gleichwertigen Leistungen nicht oder nicht in zumutbarer Weise möglich ist. Die Norm könnte bei bestimmten Apps greifen, wenn diese die einzigen sind, die jeweils die gewünschte Funktionalität anbieten.

Im Ergebnis dürfte nur in seltenen Fällen eine den Anforderungen des § 13 Abs. 2 TMG genügende Einwilligungserklärung vorliegen.

4.3 Vertragsdatenschutz

Fehlt eine wirksame Datenschutzeinwilligung kann die Datensammlung und -übertragung durch einen Erlaubnistatbestand erlaubt sein, der die Datenverarbeitung zu Vertragszwecken erlaubt. Sofern Inhalts- oder Nutzungsdaten gespeichert und übertragen werden, sind die Grenzen des § 28 Abs. 1 Satz 1 Nr. 1 BDSG und des § 15 Abs. 1 TMG zu berücksichtigen. Es dürfen die Daten verarbeitet werden, die für die Vertragserfüllung oder für die Erbringung und Abrechnung des Dienstes erforderlich sind.[27] Damit fallen Datenspeicherungen für andere Zwecke aus dem Rahmen des Zulässigen.

Nach § 15 Abs. 1 TMG gelten für Nutzungsdaten besonders strenge Anforderungen an die Zweckbindung. Sind die Nutzungsdaten nicht mehr für die jeweils aktuelle Nutzung des Dienstes erforderlich, sind sie sofort zu löschen.[28] Hierzu sind gemäß § 13 Abs. 4 Satz 1 Nr. 2 TMG technische Vorkehrungen zu treffen. Nutzungsprofile aus den nach § 15 Abs. 1 TMG erhobenen Nutzugsdaten dürfen nach § 15 Abs. 3 TMG nur unter Pseudonym erstellt werden und nicht mit dem Pseudonym zusammengeführt werden. Der Nutzer ist gemäß § 15 Abs. 3 Satz 2 TMG auf sein die Profilbildung betreffendes Widerspruchsrecht gesondert hinzuweisen. Ein solcher Hinweis fehlt in der Regel bei Apps. Die Profilbildung ist daher unzulässig. Die Profile dürften gemäß § 15 Abs. 3 Satz 3 TMG nicht mit den Daten über den Träger des Pseudonyms zusammengeführt werden. Dies ist gemäß § 13 Abs. 4 Satz 1 Nr. 6 TMG ebenfalls technisch sicherzustellen.

4.4 Einbezug der AGB

AGB können den Nutzungsvertrag weiter konkretisieren und genauer bestimmen, welche Erhebungen, Verarbeitungen und Nutzungen im Rahmen von § 15 TMG und § 28 Abs. 1 Satz 1 Nr. 1 BDSG als erforderlich anzusehen sind. Damit könnte ein umfassenderer Datenumgang ermöglicht werden. Auf den Download-Seiten der Apps finden sich aber in der Regel nur die bereits erwähnten „Datenschutzerklärungen".

Gemäß § 305 Abs. 2 Nr. 1 BGB muss der Verwender auf AGB ausdrücklich hinweisen. Es muss für seinen Vertragspartner klar und leicht erkennbar sein, dass AGB in den Vertrag einbezogen werden sollen.[29] Damit die Nutzer überhaupt erkennen könnten, dass der Inhalt von „Datenschutzerklärungen" über die üblichen Informationen hinausgeht und AGB enthält, müssten diese auch zusätzlich mit „AGB" oder ähnlich bezeichnet werden. „Datenschutzerklärungen" ohne weitere Hinweise können daher nicht als AGB Teil des Vertrags werden.

Sollten doch ausnahmsweise AGB bei einem App-Download hinterlegt sein, würden überraschende Klauseln im Sinn von § 305c BGB nicht Vertragsbestandteil. Überraschend sind Klauseln, die objektiv ungewöhnlich und subjektiv überraschend sind. Objektive Ungewöhnlichkeit liegt vor, wenn der Inhalt von AGB von dem abweicht, was ein redlicher Durchschnittskunde erwartet. Subjektiv überraschend sind Klauseln, wenn durch die erheb-

24 *Jandt/Schaar/*Schulz (Fn. 20), § 13 TMG, Rn. 83.
25 Hierzu *Spindler/Nink*, in: *Spindler/Schuster* (Fn. 9), § 13 TMG, Rn. 7.
26 S. z.B. *Schaar*, MMR 2001, 647; a.A. Simitis (Fn. 22), § 4a, Rn. 96.
27 Sehr detaillierte Beispiele zur Erforderlichkeit bei *Sachs/Meder*, ZD 2013, 303 (306).
28 *Dix/Schaar*, in: Roßnagel (Fn. 20), § 15 TMG, Rn. 54.
29 *Grüneberg*, in: *Palandt*, BGB, 61. Aufl, München 2012, § 305 BGB, Rn. 27.

liche Diskrepanz zwischen Inhalt und dem, was der Vertragspartner erwarten darf, ein Übertölpelungseffekt eintritt.[30]

Der Durchschnittskunde darf davon ausgehen, dass nur solcher Datenumgang durch AGB erlaubt wird, der zur Erfüllung des typischen Nutzungsvertrags oder zur typischen Diensterfüllung erforderlich ist, es sei denn, ein untypischer Vertrag ist klar als solcher erkennbar. Zumindest grob datenschutzwidrige Regelungen, die in keinem Zusammenhang mit der Vertragserfüllung oder Diensterbringung stehen, wären als ungewöhnlich anzusehen. Sie wären bei erheblicher Diskrepanz zur redlichen Erwartung der Durchschnittskunden auch subjektiv überraschend. Solche Klauseln könnten daher aufgrund von § 305c BGB nicht Vertragsinhalt werden und wären keine rechtliche Grundlage für einen über das üblicherweise erforderliche Maß hinausgehenden Datenumgang.

4.6 Grenzüberschreitende App-Angebote

Bei Apps, die aus dem Ausland angeboten werden, stellt sich die Frage, inwiefern deutsches Datenschutzrecht anwendbar ist. Nach § 1 Abs. 5 Satz 1 und 3 BDSG, der auch auf den TMG-Datenschutz anzuwenden ist,[31] ist das deutsche Datenschutzrecht dann anwendbar, wenn der Anbieter im Inland belegen ist und wenn ein Anbieter aus einem Drittstaat Daten im Inland erhebt, verarbeitet oder nutzt. Greift eine App eines Anbieters aus den USA auf ein Endgerät in Deutschland zu und erhebt zum Beispiel die Telefonkontakte des Nutzers vom Gerät, sind also TMG und BDSG anwendbar. In diesem Fall wäre die Rechtslage eindeutig so wie in 4.1 bis 4.3 ausgeführt.

Anders könnte der Fall zu beurteilen sein, wenn die Daten des Nutzers nicht auf dem Gerät, sondern auf einem (Cloud-) Server vorgehalten werden, der in einem Drittstaat (bspw. den USA) belegen ist, denn dann wäre wohl keine Erhebung im Inland gegeben. In diesem Fall würde z. B. US-Recht gelten, das weitere Spielräume zur Erhebung von Daten eröffnen könnte als das deutsche Recht. Bei Anbietern aus dem EU-Ausland kommt das Datenschutzrecht des jeweiligen Mitgliedstaats zur Anwendung. Dieses wird in Einzelheiten von der deutschen Rechtslage abweichen, aufgrund der gemeinsamen Datenschutzrichtlinie aber nicht zu einer generell völlig unterschiedlichen Bewertung führen.

4.7 Zusammenfassung

Das Verhalten von Apps kann gegen datenschutzrechtliche Vorgaben verstoßen. Die Rechtfertigung durch Einräumung von Berechtigungen wird in der Regel unwirksam sein, da meist gegen die Regeln der datenschutzrechtlichen Einwilligung verstoßen wird.

4.8 Rückwirkungen auf das Urheberrecht

Nach § 39 UrhG sind Änderungen des Werks zulässig, wenn der Urheber seine Einwilligung nach Treu und Glauben nicht versagen kann. § 39 UrhG schützt das Urheberpersönlichkeitsrecht.[32] Die Norm vermag im Verhältnis zu § 69 c Nr. 2 UrhG kein Änderungsrecht des Nutzers zu begründen.[33]

Für Computerprogramme sieht aber § 69d Abs. 1 UrhG eine Erlaubnis für Änderungen am Werk vor, wenn diese für den bestimmungsgemäßen Gebrauch notwendig sind. Zweck der Vorschrift ist es, dem berechtigten Nutzer des Programms die nach dem Vertrag bestimmungsgemäße Nutzung zu ermöglichen. Sie erlaubt Maßnahmen, die die fehlerfreie Ausführung des Programms sicherstellen.[34] Hierzu gehört im Rahmen der Fehlerbeseitigung auch die Entfernung von Programmfehlern und Viren.[35]

Nicht geklärt ist bisher, ob die Norm auch auf den Fall anwendbar ist, dass der Nutzer den Funktionsumfang des Programms durch Hinzufügen, Entfernen oder veränderte Interpretation von Programmcode auf den bestimmungsgemäßen Gebrauch beschränken möchte. Da rechtswidrige Funktionen aber nicht bestimmungsgemäß sind, spricht viel dafür, die Änderungen von Code, die eine rechtmäßige Nutzung der App sicherstellen, als von der Erlaubnis des § 69d Abs. 1 UrhG umfasst anzusehen.

5 Ausblick

Technischer Selbstdatenschutz ist in einer Welt, in der unübersehbar viele personenbezogene Daten erhoben und verarbeitet werden, unabdingbar, um Datenschutz zu gewährleisten.[36] Die Anwendung von Privacy Enhancing Technologies, z. B. in Form von Privacy Apps, ist in diesem Sinn die adäquate Antwort auf unerlaubte heimliche Zugriffe auf personenbezogene Daten durch bestimmte Apps. Dies ist allerdings nur dann der Fall, wenn deutsches oder EU-Datenschutzrecht anwendbar ist. Dessen Anwendungsbereich wird sich mit dem Inkrafttreten der geplanten EU-Datenschutz-Grundverordnung erweitern. Art. 3 Abs. 2 des Entwurfs der EU-Kommission erklärt dieses auch für anwendbar, wenn personenbezogene Daten einer in der Union ansässigen natürlichen Person erhoben werden, um dieser Person Waren oder Dienstleistungen anzubieten oder ihr Verhalten zu beobachten.

Dieser datenschutzrechtlich gebotene Selbstschutz kann jedoch mit dem jeweiligen nationalen Urheberrecht konfligieren, wenn er zu einer Veränderungen der Software oder ihrer Ausführung führt. In dem Beitrag wurde angedeutet, wie eine Lösung des Konflikts zwischen Datenschutz und Urheberschutz gelingen könnte.

Da sowohl die Software der App als auch der Einsatz von Privacy Apps sehr unterschiedlich gestaltet sein können, setzt eine befriedigende und in der Praxis einsetzbare Lösung noch weitere interdisziplinäre Forschung voraus.

30 Schmidt, in: *Bamberger/Roth*, BGB, 3. Aufl., München 2012, § 305c BGB, Rn. 13 ff.

31 Jotzo, MMR 2009, 232 (234).

32 *Wiebe* (Fn. 9), § 39 UrhG, Rn. 1.

33 *Grützmacher*, in: *Wandtke/Bullinger*, Urheberrecht, 3. Aufl., München 2009, § 69c UrhG, Rn. 23.

34 *Dreier* (Fn. 6), § 69d UrhG, Rn. 7 ff.

35 *Grützmacher*, (Fn. 30), § 69d UrhG, Rn. 17.

36 S. hierzu *Roßnagel*, Konzepte des Selbstdatenschutzes, in: ders., Handbuch Datenschutzrecht, 2003, S. 337 ff.