Smartphones und Apps: Datenschutzrechtliche Risiken und deren Begrenzung

Anke Brummund

Goethe-Universität Frankfurt am Main
Lehrstuhl für Öffentliches Recht, Informationsrecht, Umweltrecht und Verwaltungswissenschaften
Grüneburgplatz 1, RuW 05
60323 Frankfurt a.M.
brummund@jur.uni-frankfurt.de

Abstract: Smartphones finden heutzutage zunehmend Verbreitung, insbesondere die Zahl der heruntergeladenen zusätzlichen mobilen Anwendungen - sogenannte Apps – steigt stetig. Durch diese Entwicklung kommt es vermehrt zu Risiken für personenbezogene Daten der Smartphone-Nutzer, müssen diese im Rahmen der Installation von Apps oft in umfassende Zugriffsrechte einwilligen oder gänzlich auf die Anwendung verzichten. Dieses Alles-oder-nichts-Prinzip wird einem wirksamen Datenschutz nicht gerecht. Immer häufiger werden zudem in Tests Sicherheitsmängel bei Apps festgestellt.

Im vorliegenden Beitrag werden deshalb zunächst die datenschutzrechtlichen Risiken für Smartphone-Nutzer dargestellt und sodann einige Möglichkeiten des verstärkten Selbstdatenschutzes, inklusive einer Bewertung ihrer rechtlichen Zulässigkeit, aufgezeigt. Vorgestellt werden hierzu drei Apps: der App Permission Watcher, SRT AppGuard, sowie XPrivacy. Der Fokus liegt vornehmlich auf den beiden Letzteren, die durch Modifikationen an datenschutzrechtlich bedenklichen Apps oder dem installierten Betriebssystem ein dynamisches Rechtemanagement herstellen. Wie derartige Modifikationen urheberrechtlich zu beurteilen sind, soll im Folgenden beleuchtet werden.

1 Einführung

Smartphones haben mittlerweile sowohl für die private als auch die geschäftliche Nutzung eine hohe Bedeutung erlangt. Gerade die Möglichkeit, dem Gerät durch zusätzliche mobile Anwendungen - sogenannte Apps - individuelle, auf die jeweiligen Bedürfnisse abgestimmte Nutzungsmöglichkeiten hinzuzufügen, machen deren Gebrauch nützlich und reizvoll.[1] Diese Anwendungen bergen jedoch auch ein hohes Risiko für personenbezogene Daten, erfordern die meisten doch eine Internetverbindung und die Einwilligung in umfassende Berechtigungen.

[1] [SM13], S. 303.

Mit einer Pressemitteilung[2] vom 05.03.2014 gab das Fraunhofer-Institut für Angewandte und Integrierte Sicherheit bekannt, dass es 10.000 Android-Apps auf Sicherheitsmängel getestet habe. 91% der untersuchten Apps sollen stets eine Internetverbindung angefordert haben. Eine Installation der betroffenen Anwendungen sei nur mit Zustimmung zur Internetnutzung möglich. Eine weitaus alarmierendere Feststellung war jedoch, dass 69% der untersuchten Apps die Daten unverschlüsselt sendeten.

Durch derartige Sicherheitsmängel und die Erteilung von Berechtigungen ist eine Vielzahl von personenbezogenen Daten betroffen wie z.B. Name, Kontodaten, Adressbuchdaten, Standortdaten, Fotos und deren Metadaten, Angaben in sozialen Netzwerken usw.[3]

Einige Beispiele für mögliche Berechtigungen der Apps sind:[4]

- der Zugriff auf die Kamera oder das Mikrofon;
  denkbar dadurch sind bspw. Ton-Mitschnitte des Nutzers
- der Zugriff auf Kontaktdaten im Adressbuch
- der Zugriff auf den Standort
- der Zugriff auf E-Mail-Dienste und SMS;
  denkbar dadurch sind bspw. das Lesen und Schreiben von E-Mails/SMS

Die Menge an gesammelten Daten ist erheblich und die Tendenz weiterer Sammlung stetig steigend. Wurden 2010 ca. 386 Millionen Apps innerhalb eines Jahres in Deutschland heruntergeladen, waren es 2011 bereits rund 962 Millionen.[5] Im Jahr 2012 wurden sogar 1,7 Milliarden heruntergeladene Apps gezählt.[6] Somit zeigt sich, dass Smartphone-Apps geeignet sind, eine Vielzahl von Daten zu sammeln. Aus datenschutzrechtlicher Sicht sind sie deshalb höchstbedenklich.

Zu beachten ist außerdem, dass die durch Apps gewonnenen Daten auch teilweise bei großen Unternehmen zusammengeführt werden können. So sorgte z.B. der Kauf des Instant Messengers WhatsApp durch das soziale Online-Netzwerk Facebook für Aufse-

[2] Fraunhofer-Institut für Angewandte und Integrierte Sicherheit, Pressemitteilung vom 05.03.2014: 10000 Apps und eine Menge Sorgen, abrufbar unter: http://www.aisec.fraunhofer.de/de/medien-und-presse/pressemitteilungen/2014/20140403_10000_apps.html, [abgerufen am 26.06.2014].
[3] [SM13], S. 304.
[4] vgl. Düsseldorfer Kreis, Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter, S. 19, abrufbar unter:
http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/Orientierungshilfe_Apps_2014.pdf, [abgerufen am 26.06.2014].
[5] BITKOM, Presseinformation vom 23.02.2012: Fast eine Milliarde App-Downloads allein in Deutschland, abrufbar unter:
http://www.bitkom.org/files/documents/BITKOM-Presseinfo_Markt_Apps_in_Deutschland_23_02_2012.pdf, [abgerufen am 26.06.2014].
[6] BITKOM, Presseinformation vom 08.05.2013: Umsatz mit Apps hat sich 2012 mehr als verdoppelt, abrufbar unter:
http://www.bitkom.org/files/documents/BITKOM_Presseinfo_Apps_werden_zum_Wirtschaftsfaktor_09_05_2013.pdf, [abgerufen am 26.06.2014].

hen.[7] Die Dimension wird deutlich, wenn man beachtet, dass es sich bei WhatsApp um eine der meistgenutzten Apps[8], und bei Facebook derzeit um das weltweit größte soziale Netzwerk handelt.

Für zusätzliche Brisanz sorgte auch die Meldung, dass Geheimdienste Daten mittels Smartphone-Apps wie z.B. dem Spiel „Angry Birds", sammeln.[9]

Aufgrund dieser datenschutzrechtlichen Risiken wird Smartphone-Nutzern häufig geraten, Apps nur aus vertrauenswürdigen Quellen zu installieren sowie deren Zugriffsrechte genau zu überprüfen. Greift die Anwendung auf Daten zu, die für die eigentliche Funktion nicht erforderlich sind, so soll man demnach auf die Installation verzichten. Dies geht z.B. aus einem Ratgeber des BMWi[10] aus dem Jahre 2011 hervor.

Unter dem Aspekt, dass die Mehrheit der Apps Berechtigungen einfordert und Daten erhebt, die für die eigentliche Anwendung nicht erforderlich sind, ist dieses Alles-oder-nichts-Prinzip eine nur unbefriedigende Lösung. Zudem werden viele vertrauliche Daten unbemerkt übermittelt, ohne dass der Smartphone-Nutzer davon Kenntnis erlangt.[11] Ein Verzicht auf die Installation ist dem Nutzer in solchen Fällen mangels Informiertheit erst gar nicht möglich.

Es besteht deshalb ein starker Bedarf an alternativen Lösungen. Die ledigliche Möglichkeit einer pauschalen Einwilligung in die Zugriffsrechte wird kritisiert und der Wunsch nach einer Stärkung des Selbstdatenschutzes durch individuelle Steuerungsmöglichkeiten laut.[12]

Zwischenzeitlich wurden diverse Anwendungen entwickelt, um problematische Apps aufzuspüren und gegebenenfalls anzupassen. Diese lassen sich im Wesentlichen in drei Kategorien einteilen: Anwendungen, die das Überwachen von Apps ermöglichen (2.1), solche, die kritische Apps selbst verändern (2.2), und Apps, die der Modifikation des Betriebssystems dienen (2.3), um sodann auf die kritische Anwendung einzuwirken. Diese Kategorien sollen im Folgenden an Hand jeweils einer konkreten Anwendung vorgestellt und deren urheberrechtliche Zulässigkeit mit Blick auf die erfolgten Modifikationen überprüft werden.

---

[7] Heise Online vom 19.02.1014, Facebook kauft WhatsApp, abrufbar unter: http://heise.de/-2118920, [abgerufen am 26.06.2014].
[8] vgl. [Kr12], S. 438.
[9] Süddeutsche vom 27.01.2014, Apps im Fokus von NSA und GCHQ – Angry Birds in Überwachungsmission, abrufbar unter: http://sz.de/1.1873548, [abgerufen am 26.06.2014].
[10] BMWi, Mobile Sicherheit – Ortung – Datenschutz, abrufbar unter: https://www.bsi-fuer-buerger.de/SharedDocs/Downloads/DE/BSIFB/Publikationen/extern/Mobile-Sicherheit-Ortung-Datenschutz.pdf?__blob=publicationFile, [abgerufen am 26.06.2014].
[11] [Ha11].
[12] Düsseldorfer Kreis, Beschluss vom 04/05. Mai 2011, Datenschutzgerechte Smartphone-Nutzung ermöglichen, S. 1 f., abrufbar unter: https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/Inhalt/2011/Datenschutzgerechte_Smartphone-Nutzung_ermoeglichen_/Datenschutzgerechte_Smartphone-Nutzung_erm__glichen_.pdf, [abgerufen am 26.06.2014].

2 Schutzmöglichkeiten

2.1 Der App Permission Watcher

Bei dem App Permission Watcher (deutsch: App-Berechtigungswächter) handelt es sich um eine Anwendung, die es dem Smartphone-Nutzer ermöglicht, Zugriffsrechte von installierten Apps einzusehen und zu überprüfen.

Unter anderem ermöglicht die Anwendung folgende Funktionen:[13]

- die Anzeige verdächtiger Apps
- die Anzeige aller systemfremden Apps
- die Anzeige aller Berechtigungen und von welchen Apps diese genutzt werden
- die Möglichkeit bestimmte Apps als vertrauenswürdig zu markieren: diese werden danach nicht mehr als verdächtig gemeldet

Eine solche Anwendung ist zwar durchaus nützlich und wünschenswert, um Apps auf dem Smartphone regelmäßig zu überwachen, jedoch wird auch dadurch nicht das unbefriedigende Alles-oder-nichts-Prinzip beseitigt, da die Anwendung zwar die Analyse, nicht aber die Beschränkung von Zugriffsrechten einzelner Apps ermöglicht. Ein dynamisches Rechtemanagement wird so nicht hergestellt. Urheberrechtlich relevante Modifikationen finden nicht statt, gleichzeitig begrenzt dies jedoch auch die Effizienz des Selbstdatenschutzes mithilfe des App Permission Watchers.

2.2 Die Modifikation von Apps am Beispiel des SRT AppGuards

Der SRT AppGuard ist ein Beispiel für eine Anwendung, deren Funktion darin liegt, das Rechtemanagement von Apps zu überwachen und im Falle von Sicherheitsmängeln die jeweilige Anwendung zu deinstallieren, modifizieren und in neuer Version zu installieren. Die Kernaufgabe liegt also im Verändern der App selbst, das auf dem Smartphone installierte Betriebssystem bleibt unberührt.

Vorteil dieser Anwendung ist, dass es dem Benutzer so auf gewissermaßen einfache Art und Weise möglich ist, einzelne Berechtigungen durch Entfernen der jeweils daneben stehenden Häkchen zu entziehen und ein dynamisches Rechtemanagement herzustellen. Die unerwünschten Zugriffsrechte werden sodann blockiert. Dies birgt jedoch auch den Nachteil, dass es zu Funktionsproblemen und Abstürzen einer App kommen kann, sollte die Anwendung ohne die entzogenen Zugriffsrechte nicht mehr funktionsfähig sein.

Einige Wochen lang war der SRT AppGuard im Google Play Store zum Herunterladen bereitgestellt, wurde nach kurzer Zeit aber wieder entfernt und kann momentan nur über die Internetseite des Anbieters heruntergeladen werden.[14] Mögliche Ursache hierfür ist,

[13] App Permission Watcher, Informationen, abrufbar unter: http://www.apewatch.de/index_de.html, [abgerufen am 26.06.2014].
[14] Heise Online vom 05.07.2012, AppGuard: Kontrolle ungewollter App-Berechtigungen unter Android, abrufbar unter: http://heise.de/-1632532, [abgerufen am 26.06.2014].

dass Google die Anwendung als Verstoß gegen seine Google Play Nutzungsbedingungen[15] sah. Unter „6. Rechte und Einschränkungen“ werden darin Eigentumshinweise gegeben, nach denen es App-Käufern nicht gestattet ist, zu „versuchen, über Google Play erhaltene Inhalte zu verändern, einschließlich aller Veränderungen zum Zweck des Verbergens oder Änderns von Angaben zur Eigentümerschaft oder Herkunft von Inhalten“.

Eine wesentlich bedeutendere Frage ist jedoch, ob das Modifizieren der App eine Urheberrechtsverletzung darstellt.

2.2.1 Technische Grundlagen der Modifikation von Apps

Technisch erfolgt die Modifikation der Anwendung, indem dem Bytecode ein weiterer Programmcode – die sogenannte Sicherheitsbibliothek - hinzugefügt und die App anschließend neu installiert wird.[16]

Anwendungen für Android werden in der Regel in der Programmiersprache Java geschrieben.[17] Dieser zunächst erstellte Quellcode ist für Menschen lesbar, nicht jedoch von Computern bzw. Prozessoren ausführbar, da diese nur sogenannte Maschinencodes - Abfolgen aus Nullen und Einsen - ausführen können. Es bedarf deshalb der Übersetzung des Quellcodes, z.B. mittels javac. Diesen Vorgang bezeichnet man als Kompilieren.[18] Im Falle von Java besteht die Besonderheit darin, dass durch das Kompilieren nicht direkt der Maschinencode, sondern ein Zwischencode - der sogenannte Bytecode - erstellt wird. Dieser ist weder von Menschen lesbar, noch von Computern ausführbar.

In einem weiteren Schritt kann der Bytecode dann mittels eines Interpreters, z.B. Java Run Time, für den Prozessor in einen Maschinencode übersetzt und ausführbar gemacht werden.[19] Der Vorteil davon liegt in der Plattformunabhängigkeit, da der Bytecode auf allen Betriebssystem und jeder Hardware mit installierter Java Virtual Machine ausgeführt werden kann.

2.2.2 Urheberrechtliche Bewertung der Modifikation von Apps

Wird dem Zwischencode ein weiterer Programmcode hinzugefügt, um die Berechtigungen zu verändern, so könnte dem Urheber der App-Software eventuell ein Unterlassungs- und/oder Schadensersatzanspruch nach § 97 Abs. 1 UrhG zustehen. Zudem wäre ein Vernichtungsanspruch nach § 98 Abs. 1 UrhG denkbar.

---

[15] Google Play Nutzungsbedingungen, Stand vom 08.04.2014, abrufbar unter: https://play.google.com/intl/de_de/about/play-terms.html, [abgerufen am 26.06.2014].
[16] SRT AppGuard, Benutzerhandbuch, S. 18, abrufbar unter: http://apps.backes-srt.com/appguard/wp-content/uploads/sites/2/2014/03/AppGuard_Benutzerhandbuch.pdf, [abgerufen am 26.06.2014].
[17] [Ko12], S. 24 und S. 47.
[18] [LM06], S. 46.
[19] [LM06], S. 12.

2.2.2.1 Schutzgegenstand nach § 69a UrhG

Gemäß § 69a UrhG genießen auch Computerprogramme den Schutz des Urheberrechtsgesetzes. Der Begriff Computerprogramm wurde in § 1 (i) der Mustervorschriften für den Schutz von Computersoftware definiert als „Folge von Befehlen [...], die nach Aufnahme in einen maschinenlesbaren Träger fähig sind zu bewirken, dass eine Maschine mit informationsverarbeitenden Fähigkeiten eine bestimmte Form oder Aufgabe oder ein bestimmtes Ergebnis anzeigt, ausführt oder erzielt“.[20] Diese Definition wurde insoweit von der Literatur und Rechtsprechung übernommen.[21] Die Bundesregierung entschied sich aufgrund schneller technischer Entwicklungen gegen eine gesetzliche Definition.[22]

Der Bytecode ist eine Folge von Befehlen, die nach weiterer Übersetzung ein bestimmtes Ergebnis haben, nämlich die App ausführen. Es kommt für einen urheberrechtlichen Schutz nach § 69a UrhG weder auf die Programmiersprache an noch darauf, in welchem Code das Programm vorliegt. Es können auch Quellcodes, Maschinencodes, sowie der hier relevante Objektcode geschützt sein[23], obwohl dieser nur maschinell lesbar ist.[24] Der Bytecode ist dem Schutzgegenstand also grundsätzlich zuzuordnen.

Ob jeweils die Schutzvoraussetzungen von § 96a Abs. 3 UrhG vorliegen, nämlich eine ausreichende geistige Schöpfung des Urhebers, muss grundsätzlich im Einzelfall gesondert entschieden werden. Bei größeren Computerprogrammen kann jedoch in der Regel davon ausgegangen werden, da die Anforderungen an die Schöpfungshöhe seit Verabschiedung der EU-Richtlinie zum Computerprogrammschutz deutlich gesenkt wurden. Auch die Gesetzesbegründung weist ausdrücklich darauf hin, dass der Urheberrechtsschutz die Regel, die fehlende Schöpfungshöhe die Ausnahme sein soll.[25] Außerdem ist hinzuzufügen, dass durch Veränderungen des Bytecodes die Ausführung der gesamten Anwendung verändert werden kann.

2.2.2.2. Zustimmungsbedürftigkeit nach § 69c Nr. 2 UrhG

Kommt man deshalb zu dem Schluss, dass die vom SRT AppGuard modifizierten Apps von § 69a UrhG erfasst werden, so stellt sich ein beachtliches Problem für Smartphone-Nutzer im Rahmen ihres Selbstdatenschutzes. Bei der Modifikation handelt es sich um eine Umarbeitung der App, die nach § 69c Nr. 2 UrhG grundsätzlich zustimmungsbedürftig ist, da eine sonstige Programmänderung wie Erweiterung, Einschränkung und Ergänzung des Funktionsumfangs ausreicht, um eine Umarbeitung zu bejahen.[26] Das ausschließliche Recht dazu liegt lediglich beim Rechtsinhaber. Das ist aber nicht der Käufer der jeweiligen App, sondern der Urheber selbst.[27] Der App-Nutzer erwirbt durch den Kauf der jeweiligen Anwendung nicht das Urheberrecht an der selbigen, sondern nur

[20] Denkschrift über den Rechtsschutz der Datenverarbeitungssoftware, GRUR 1979, S. 306.
[21] [Sc11], S. 1086.
[22] BT-Drs. 12/4022, S. 9.
[23] [DS13], § 69a Rn. 12.
[24] [Sc13], Rn. 209.
[25] BT-Drs. 12/4022, S. 9.
[26] [DS13], § 69c Rn. 16.
[27] [Bo13], S. 722.

eine Nutzungslizenz. Eine Zustimmung wäre demnach erforderlich, die in der Regel aber fehlt.

Etwas anderes ergäbe sich nur, wenn es sich bei der App um eine Open Source Anwendung handelte. Anders als bei Closed Source-Software sind bei solcher Software Veränderungen und Weiterentwicklungen in der Regel gestattet.[28] Der Urheber verzichtet hierbei nicht vollständig auf seine Rechte, sondern es erfolgen die Übertragung eines nichtausschließlichen Nutzungsrechts für jedermann sowie die Überlassung des Quellcodes. Umarbeitungen sind gestattet, sofern sie ebenfalls nichtproprietär weitergegeben werden. Im Falle von Zuwiderhandlungen erlischt das nichtausschließliche Nutzungsrecht.[29] Ob eine App als Closed oder Open Source-Software konzipiert wurde und welchem Lizenzmodell sie unterliegt, muss im Einzelfall geprüft werden.[30] Festgestellt werden kann jedoch, dass proprietäre Software urheberrechtliche Probleme beim Selbstdatenschutz auslösen kann.

2.2.2.3 Keine Zustimmungsbedürftigkeit aufgrund von § 69d Abs. 1 UrhG

Um Smartphone-Nutzern einen besseren Schutz ihrer Daten zu ermöglichen, kam deshalb in der Literatur der Gedanke auf, ob § 69d Abs. 1 UrhG in diesem Fall eine Zustimmungsbedürftigkeit ausschließt.[31] Dazu müsste die Modifikation der Anwendung notwendig sein, um eine bestimmungsgemäße Benutzung der App zu ermöglichen.

Der Begriff „bestimmungsgemäße Benutzung“ unterliegt keiner gesetzlichen Definition. Was darunter zu verstehen ist, ist von den jeweiligen vertraglichen Vereinbarungen abhängig.[32] Erfordert eine App Berechtigungen, so wird der Käufer im Rahmen der Installation angehalten, in derartige Zugriffsrechte einzuwilligen. Bezüglich nichterforderlicher Berechtigungen gilt dies zunächst ebenso wie für Zugriffsrechte, die für die Funktionsfähigkeit der App zwingend erforderlich sind. Zu beachten ist aber auch, dass der App-Nutzer entweder in sämtliche Berechtigungen einwilligen oder gänzlich auf die App verzichten muss. Das entspricht dem heute gängigen Geschäftsmodell von „Leistung gegen Daten“.[33] Somit darf keinesfalls zweifelsfrei angenommen werden, dass der Zugriff auf kritische Daten stets vertraglich vereinbart wurde, denn eine Einwilligung bedarf zu ihrer Wirksamkeit unter anderem der Freiwilligkeit und Informiertheit. Besonders die Informiertheit ist aber problematisch, erfordert diese doch, dass der Nutzer im Voraus über den Zweck unterrichtet werden und er in der Regel genaue Kenntnis von den Umständen der Erhebung, Verarbeitung oder Nutzung der Daten erlangen muss.[34]

Bei Smartphone-Anwendungen werden derartige Kriterien in der Regel nicht erfüllt. In den meisten Fällen kommt man für nichterforderliche Berechtigungen deshalb zu dem Schluss, dass die Einwilligung als unwirksam anzusehen ist. In diesem Falle ist die ver-

[28] [DS13], § 69a Rn. 11.
[29] [DS13], § 69c Rn. 38.
[30] vgl. [BE13], S. 110 f.
[31] befürwortend: [Bo13], S. 725.
[32] [AG14], § 69d Rn. 5.
[33] [Bu10], S. 41.
[34] [BE13], S. 67.

tragliche Vereinbarung unwirksam und somit nicht vom bestimmungsgemäßen Gebrauch erfasst.

Fehlt es an einer Vereinbarung, muss sodann auf die übliche Nutzung abgestellt werden.[35] Zwar sind Smartphone-Apps in der Regel datenschutzrechtlich bedenklich, dies lässt jedoch nicht die Schlussfolgerung zu, dass die gewöhnliche Nutzung auch die rechtswidrige Erfassung von personenbezogenen Daten umfasst. Vielmehr wurde nur wirksam vereinbart, dass diejenigen Zugriffsrechte zulässig sind, die für die Funktionsfähigkeit der App erforderlich sind. Dieser Gedanke kann auch § 306 Abs. 1 BGB entnommen werden. Modifiziert der App-Nutzer nun mithilfe des SRT AppGuards die Zugriffsrechte auf das Erforderliche, so beschränkt er die Berechtigungen praktisch auf den bestimmungsgemäßen Gebrauch.[36] Von der Bedeutung des Begriffes wären derartige Modifikationen also durchaus erfasst.

Es stellt sich jedoch weiter die Frage, ob eine Beschränkung auf den bestimmungsgemäßen Gebrauch auch notwendig ist. Es reicht nicht aus, dass eine derartige Umarbeitung nützlich oder zweckmäßig scheint.[37] Stellt man jedoch fest, dass ohne eine Beschränkung der Zugriffsrechte auf das Erforderliche - mangels wirksamer Vereinbarung - bei der Nutzung der App stets eine Verletzung des Allgemeinen Persönlichkeitsrechts stattfindet und keine rechtmäßige Datennutzung vorliegen kann, so sind die Modifikationen keineswegs nur nützlich. Vielmehr besteht nur die Möglichkeit, diese Umarbeitungen vorzunehmen, soll der App-Entwickler Daten nicht rechtswidrig nutzen dürfen.

Um dem Selbstdatenschutz gerecht zu werden, erscheint es deshalb sachgerecht, § 69d Abs. 1 UrhG und den bestimmungsgemäßen Gebrauch weit auszulegen. Zwar gewähren die App-Anbieter ihre Anwendungen in der Regel nur deshalb kostenlos, um im Gegenzug die angefragten Daten zu erhalten, dieses Interesse überwiegt aber keineswegs das an dem Schutz der personenbezogenen Daten eines Smartphone-Nutzers.

2.2.3 Zwischenergebnis

Da nach § 69d Abs. 1 UrhG die Zustimmungsbedürftigkeit entfällt, sind Ansprüche nach den §§ 97 ff. UrhG also in der Regel nicht denkbar. Um Smartphone-Nutzern hier eine sichere Rechtslage gewährleisten zu können und sich nicht lediglich auf eine weite Auslegung stützen zu müssen, sollte eine ausdrückliche Regelung im Gesetz aufgenommen werden.

2.3 Die Modifikation von Betriebssystemen am Beispiel von XPrivacy

Bei XPrivacy handelt es sich ebenfalls um eine Anwendung, die dem Nutzer ein dynamisches Rechtemanagement ermöglicht. Der Smartphone-Nutzer kann auch hier mithilfe der Anwendung Berechtigungen von Apps beschränken, indem er sich deren Zugriffsrechte anzeigen lässt, um sodann durch Entfernen der jeweiligen Häkchen die Berechti-

[35] [AG14], § 69d Rn. 5.
[36] vgl. [Bo13], S. 725.
[37] [DS13], § 69d Rn. 11.

gung zu entziehen. Zudem gibt die Anwendung Auskunft darüber, welche Daten bereits von der App verwendet wurden. Als Folge der individuellen Einstellungen des Nutzers blockiert XPrivacy in den meisten Fällen jedoch nicht das Senden von Daten per se, sondern übermittelt entweder falsche Informationen wie z.B. einen anderen Standort oder leere Datensätze wie z.B. eine leere Kontaktliste, um dem Schutz personenbezogener Daten gerecht zu werden.[38] Hierin liegt ein Vorteil im Vergleich zum SRT AppGuard, da somit mangels blockierter Zugriffsrechte eine nahezu reibungslose Funktionsfähigkeit der App sichergestellt wird. Die Anwendung ist deshalb unter datenschutzrechtlichen Gesichtspunkten eine effektive Schutzmöglichkeit.

2.3.1 Technische Grundlagen der Modifikation von Betriebssystemen

Um XPrivacy nutzen zu können, bedarf es jedoch der vollen Zugriffs- und Schreibrechte auf dem Smartphone. Diese erlangt man via „Root“ bei Android bzw. „Jailbreak“ bei Apple iOS.[39] Hierunter versteht man die Modifikation des Betriebssystems, um sodann Administratorrechte zu erhalten. Das Rootkonto ist also ein Superuserkonto, das dem Nutzer auch ermöglicht, Kernfunktionen zu verändern. Bei „Root“ und „Jailbreak“ handelt es sich im Wesentlichen lediglich um verschiedene Begrifflichkeiten für dasselbe.[40] Der Nachteil besteht für den durchschnittlichen Smartphone-Nutzer jedoch in der Erforderlichkeit gewisser technischer Kenntnisse und der Entstehung von Risiken. So sind mobile Endgeräte nach dem „Rooten“ durchaus anfälliger für Malware, und es mangelt an Updates. Zudem können Schäden am Smartphone entstehen, sodass dessen Funktionsfähigkeit verlustig gehen kann („bricked device“[41]). Ein weiterer Nachteil liegt darin, dass viele Hersteller nach derartigen Eingriffen die Garantie versagen und man sich lediglich auf die normalen Gewährleistungsansprüche berufen kann.[42]

2.3.2 Urheberrechtliche Bewertung der Modifikation von Betriebssystemen

In beiden Fällen wird zunächst das Betriebssystem modifiziert, um sodann die betroffene Anwendung zu installieren. Dies wirft erneuert urheberrechtliche Fragestellungen auf, denn auch Firmware wie Android und Apple iOS ist von den §§ 69a ff. UrhG erfasst, sodass die Modifikation via „Root“ oder „Jailbreak“ eine Umarbeitung nach § 69c Nr. 2 UrhG darstellt.

Hier ist jedoch zwischen der Open Source-Software Android und der Closed Source-Software Apple iOS zu unterscheiden.

---

[38] vgl. Beschreibung des Google-Play-Stores, abrufbar unter: https://play.google.com/store/apps/details?id=biz.bokhorst.xprivacy.installer&hl=de, [abgerufen am 26.06.2014].
[39] Chip Online vom 09.12.2013, Android rooten: Vorteile und Nachteile, abrufbar unter: http://www.chip.de/news/Android-rooten-Vorteile-und-Nachteile_62681106.html, [abgerufen am 26.06.2014].
[40] [KK12], S. 100.
[41] [KK12], S. 99.
[42] [KK12], S. 101.

2.3.2.1 Android

Bei der Open Source-Software Android folgen aus der Umarbeitung keine besonderen urheberrechtlichen Probleme, da derartige Modifikationen von der Apache Software License, Version 2.0[43], erfasst sind.[44]

2.3.2.2 Apple iOS

Bei Apple iOS stellen sich derartige Umarbeitungen jedoch anders dar, da es sich hier um eine Closed Source-Software handelt. Es fehlt an einer Zustimmung zur Umarbeitung nach § 69c Nr. 2 UrhG. Hier kann auch keine Lösung über § 69d Abs. 1 UrhG getroffen werden, da der Smartphone-Nutzer durch „Jailbreak" nicht das Betriebssystem auf den bestimmungsgemäßen Gebrauch beschränken muss, um sich vor rechtswidriger Datennutzung durch die Firmware zu schützen. Vielmehr geht es beim „Jailbreak" erst in einem weiteren Schritt um den Selbstdatenschutz, nämlich sobald der Programmablauf der Anwendungen verändert wird. Die Veränderung des Betriebssystems iOS stellt demnach nach deutschem Recht eine Urheberrechtsverletzung dar, die Ansprüche nach §§ 97 ff. UrhG nach sich ziehen kann. Lediglich § 108b UrhG ist bei Modifikationen zum privaten Gebrauch nicht anwendbar.

In den USA wurde „Jailbreak" vor allem 2010 thematisiert und vorübergehend eine Ausnahmeregelung vom Digital Millenium Copyright Act beschlossen. Auch im US-amerikanischen Recht ist eine Umgehung von technischen Maßnahmen zum Urheberschutz grundsätzlich verboten (Section 1201(a)(1)(A) des Digital Millenium Copyright Act[45]). Gemäß Section 1201(a)(1)(C)[46] legt jedoch der Librarian of Congress, auf Empfehlung des Register of Copyrights, alle drei Jahre Ausnahmeregelungen für bestimmte Handlungen fest, sodass gewisse Umgehungen von Zugangsbeschränkungen für drei Jahre als legal anzusehen sind. Im Jahre 2010 wurde „Jailbreak" als eine solche Ausnahme aufgenommen.[47] Eine vergleichbare Diskussion fand in Deutschland bisher nicht in diesem Maße statt, sodass es an gleichwertigen Regelungen fehlt.

---

[43] Die Version 2.0 ist abrufbar unter: http://www.apache.org/licenses/LICENSE-2.0, [abgerufen am 26.06.2014].

[44] vgl. Android Licenses, abrufbar unter: https://source.android.com/source/licenses.html, [abgerufen am 26.06.2014].

[45] "§ 1201 (a) Violations Regarding Circumvention of Technological Measures. — (1)(A) No person shall circumvent a technological measure that effectively controls access to a work protected under this title. The prohibition contained in the preceding sentence shall take effect at the end of the 2-year period beginning on the date of the enactment of this chapter."

[46] "§ 1201 (a) Violations Regarding Circumvention of Technological Measures. — (1)(C) During the 2-year period described in subparagraph (A), and during each succeeding 3-year period, the Librarian of Congress, upon the recommendation of the Register of Copyrights, who shall consult with the Assistant Secretary for Communications and Information of the Department of Commerce and report and comment on his or her views in making such recommendation, shall make the determination in a rulemaking proceeding for purposes of subparagraph (B) of whether persons who are users of a copyrighted work are, or are likely to be in the succeeding 3-year period, adversely affected by the prohibition under subparagraph (A) in their ability to make noninfringing uses under this title of a particular class of copyrighted works."

[47] Federal Register, Vol. 75, No. 143/Tuesday, July 27, 2010/Rules and Regulations, III. B. "Computer programs that enable wireless telephone handsets to execute software applications, where circumvention is ac-

Abgesehen von den urheberrechtlichen Problemen der Modifikation von iOS selbst, stellt auch die Einwirkung des gerooteten Smartphones auf die Programmabläufe von Apps eine urheberrechtlich relevante Handlung dar, obwohl in diesem Fall keine Modifikation des Bytecodes erfolgt. Laut OLG Hamburg ist keine Veränderung der Programmsubstanz erforderlich.[48] Es genüge, wenn durch externe Befehle in die Ausführung und den Ablauf eingegriffen werde. Der Begriff Umarbeitung sei weit auszulegen.[49] Durch diese weite Auslegung werden Rechtslücken durch technische Neuerungen vermieden. So stellt auch das Ausführen von XPrivacy grundsätzlich eine zustimmungsbedürftige Handlung nach § 69c Nr. 2 UrhG dar. Es ist jedoch auch hier wieder § 69d Abs. 1 UrhG zu beachten, da in diesem Fall die Anwendung auf den bestimmungsgemäßen Gebrauch beschränkt wird, was bei rechtswidriger Datenerhebung notwendig ist. Hier kann auf die Ausführungen zum SRT AppGuard verwiesen werden.

2.3.3 Zwischenergebnis

Ansprüche nach §§ 97 ff. UrhG kommen also nur wegen der Umarbeitung der Firmware iOS in Betracht, nicht jedoch hinsichtlich der Einwirkung von XPrivacy auf den Ablauf der betroffenen App. Schadensersatzansprüche als Folge der Umarbeitung der Firmware sind allerdings wenig wahrscheinlich, da die zuverlässige Berechnung der Schadenshöhe meist nicht möglich sein dürfte.[50] Unterlassungs- und Vernichtungsansprüche sind hingegen denkbar.

3 Fazit und Ausblick

Zusammenfassend lässt sich feststellen, dass es zwar bereits Möglichkeiten gibt, den Selbstdatenschutz von Smartphone-Nutzern zu verbessern, diese jedoch zum einen für den durchschnittlichen Bürger nur schwer durchführbar sind, und zum anderen zu Urheberrechtsverletzungen führen können.

So erfordern die jeweiligen Mechanismen gewisse technische Kenntnisse, die nicht von jedermann erwartet werden können. Dies gilt insbesondere bei Anwendungen wie XPrivacy, die Modifikationen am Betriebssystem erfordern. Bei nicht ausreichender technischer Kenntnis kann es hier zu riskanten Beschädigungen kommen.

---

complished for the sole purpose of enabling interoperability of such applications, when they have been lawfully obtained, with computer programs on the telephone handset", S. 43828, abrufbar unter: http://www.copyright.gov/fedreg/2010/75fr43825.pdf, [abgerufen am 26.06.2014]; vgl. The Center for Internet and Society at Stanford Law School, Library of Congress: Fair use lets you jailbreak your iPhone, abrufbar unter: http://cyberlaw.stanford.edu/blog/2010/07/library-congress-fair-use-lets-you-jailbreak-your-iphone, [abgerufen am 26.06.2014].

[48] OLG Hamburg, Urteil vom 13.04.2012 – AZ 5 U 11/11, GRUR-RR 2013, S. 13.

[49] OLG Hamburg, Urteil vom 13.04.2012 – AZ 5 U 11/11, GRUR-RR 2013, S. 15.

[50] Gäfgen, Jailbreak, Root und Custom-Rom für Android und iOS legal oder nicht? Rechtslage kommentiert mit Fallbeispielen, PCGamesHardware.de vom 21.03.2012, abrufbar unter: http://www.pcgameshardware.de/Panorama-Thema-233992/Specials/Jailbreak-iphone-4s-ipad-3-Root-Custom-rom-873885/4/, [abgerufen am 26.06.2014].

Bezüglich Apple iOS ist zudem hinzuzufügen, dass derartige Modifikationen an der Firmware nach deutschem Recht eine Urheberrechtsverletzung darstellen.

Bei der Anwendung SRT AppGuard liegt der Vorteil zwar in den geringeren notwendigen Kenntnissen und der fehlenden Urheberrechtsverletzung hinsichtlich der Firmware, da keine Modifikation am Betriebssystem vorgenommen werden muss, sie blockiert jedoch die Zugriffsrechte per se und kann so zur vollständigen Funktionsunfähigkeit der modifizierten App führen. Dies entspricht nicht dem Ziel eines effektiven Selbstdatenschutzes. Zudem ist die Rechtslage bezüglich urheberrechtlicher Fragestellungen bei der Modifikation an datenschutzunfreundlichen Apps nicht ausreichend geklärt. Es bedarf deshalb einer gesetzlichen Klarstellung, dass derartige Umarbeitungen von § 69d UrhG als umfasst gelten, um Smartphone-Nutzern Rechtssicherheit zu verschaffen und die Motivation zum Selbstdatenschutz zu stärken.

Literaturverzeichnis

[AG14] Ahlberg, H.; Götting, H.-P.: Beck'scher Online-Kommentar Urheberrecht, München, Stand 01.02.2014.

[BE13] Baumgartner, U.; Ewald, K.: Apps und Recht, München, 2013.

[Bo13] Bodden, E.; Rasthofer, S.; Richter, P.; Roßnagel, A.: Schutzmaßnahmen gegen datenschutzunfreundliche Smartphone-Apps – Technische Möglichkeiten und rechtliche Zulässigkeit des Selbstdatenschutzes bei Apps, in: Datenschutz und Datensicherheit 2013, S. 720-725.

[Bu10] Buchner, B.: Die Einwilligung im Datenschutzrecht – vom Rechtfertigungsgrund zum Kommerzialisierungsinstrument, in: Datenschutz und Datensicherheit 2010, S. 39-43.

[DS13] Dreier, T.; Schulze, G.: Urheberrechtsgesetz: UrhG - Urheberrechtswahrnehmungsgesetz, Kunsturhebergesetz Kommentar, 4. Auflage, München, 2013.

[Ha11] Haag, N.: iPhone – Apps übermitteln unbemerkt vertrauliche Daten, MultiMedia und Recht-Aktuell 315048.

[KK12] Kersten, H.; Klett, G.: Mobile Device Management, Heidelberg, 2012.

[Ko12] Koppay, H.: Die Entwicklung und Vermarktung von Handy-Apps – Einstieg in die Welt der mobilen Applikationen, Hamburg, 2012.

[Kr12] Kremer, S.: Datenschutz bei Entwicklung und Nutzung von Apps für Smart Devices, in: Computer und Recht 2012, S. 438-446.

[LM06] Louis, D.; Müller, P.: Java 5 – Easy: Aufregend Programmieren, München, 2006.

[Sc11] Schwartmann, R.: Praxishandbuch Medien-, IT- und Urheberrecht, 2. Auflage, Heidelberg, 2011.

[Sc13] Schack, H.: Urheber- und Urhebervertragsrecht, 6. Auflage, Tübingen, 2013.

[SM13] Sachs, A.; Meder, M.: Datenschutzrechtliche Anforderungen an App-Anbieter, Prüfungen am Beispiel von Android-Apps, in: Zeitschrift für Datenschutz 2013, S. 303-308.