Karlsruher Institut für Technologie

AVARE Projektbericht
1. Meilenstein

Open Access am KIT

von Sascha Alpers[1], Stefanie Betz[2], Andreas Fritsch[2], Andreas Oberweis[2], Maria Pieper[1], Gunther Schiefer[2], Manuela Wagner[3]

KIT SCIENTIFIC WORKING PAPERS 50

[1] FZI Forschungszentrum Informatik
[2] Institut für Angewandte Informatik und Formale Beschreibungsverfahren
[3] Zentrum für Angewandte Rechtswissenschaft

Das Projekt wird von der Baden-Württemberg Stiftung gGmbH im Rahmen des Forschungsprogramms „IKT-Sicherheit“ finanziert. Projektträger ist das DLR.

www.privacy-avare.de

Projektkoordinator

Karlsruher Institut für Technologie (KIT)
Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB)
Dr. Stefanie Betz
Kaiserstraße 12
76131 Karlsruhe
www.aifb.kit.edu

Projektpartner

Karlsruher Institut für Technologie (KIT)
Zentrum für Angewandte Rechtswissenschaft (ZAR)
Dr. Oliver Raabe
Vincenz-Prießnitz-Straße 3
76131 Karlsruhe
www.zar.kit.edu

FZI Forschungszentrum Informatik
Forschungsbereich SE Software Engineering
Sascha Alpers
Haid- und Neu-Straße 10-14
76131 Karlsruhe
www.fzi.de

Impressum

Karlsruher Institut für Technologie (KIT)
www.kit.edu

2016

ISSN: 2194-1629

Inhalt

1 Einleitung 2

2 Grundlagen 3

2.1 Technische Grundlagen 3

2.2 Rechtliche Grundlagen 3

2.2.1 Anwendbarkeit des deutschen Rechtsrahmens 3

2.2.2 Verantwortliche Stelle 4

2.2.3 Legitimation im nationalen Datenschutzrecht 6

2.2.4 Kollisionen mit Datenschutzprinzipien 7

2.2.5 Datenschutzrechtliche Risiken des Webtrackings 17

3 Existierende Softwareanwendungen 18

3.1 Arbeitsweise der untersuchten Datenschutz-Apps 19

3.2 Benutzbarkeit der untersuchten Datenschutz-Apps 20

3.3 Funktionalität der untersuchten Datenschutz-Apps 21

3.4 Detaillierte Beschreibung ausgewählter Datenschutz-Apps 25

3.4.1 SRT AppGuard 25

3.4.2 Advanced Permission Manager 25

3.4.3 LBE Security Master 26

3.4.4 XPrivacy 27

3.5 Rechtliche Implikationen 28

3.5.1 Urheberrecht 28

3.5.2 Vertragsrecht 33

4 Zusammenfassung und Ausblick 33

4.1 Kommende Rechtslage 33

4.1.1 Das „Eigentum“ an Daten 33

4.1.2 Das Geschäftsmodell „Dienst gegen Daten“ 35

4.1.3 Ausblick 36

4.2 Gesamtbewertung der existierenden Softwareanwendung 37

5 Literaturverzeichnis 38

6 Anhang 42

6.1 Desktopbasierte Analysetools 42

6.2 Manifest-Datei (Beispiel) 42

1 Einleitung

Das Projekt „Anwendung zur Verteilung und Auswahl rechtskonformer Datenschutzeinstellungen“ (kurz AVARE) hat das Ziel die Datensouveränität der einzelnen Bürgerinnen und Bürger zu stärken.

Unser Alltag wird immer stärker von global vernetzter Informations- und Kommunikationstechnologie (IKT) geprägt. Besonders die allgegenwärtige Vernetzung führt dazu, dass Unternehmen, Organisationen und private Haushalte permanent online sind, wodurch sowohl das Zusammen- als auch das Geschäftsleben sowie die Kommunikation im Allgemeinen stark verändert werden. Smartphones, digitale Soziale Netzwerke, kommerzielle Rabattsysteme, Cloud-Anwendungen und Ubiquitous Computing führen zur verstärkten Preisgabe personenbezogener Informationen. Diese Informationen werden teils ohne das Wissen der Bürger von multinationalen Konzernen gesammelt, gespeichert, ausgewertet und verwertet. Bürger können in diesem komplexen Szenario den Schutz Ihrer Daten nur schwer durchsetzen. Auch wird es immer schwerer nachzuvollziehen, wo und durch wen die eigenen Nutzerdaten verarbeitet und verwendet werden.

Ziel des AVARE Projektes ist es daher, die Bürger beim Schutz ihrer personenbezogenen Daten durch eine innovative und nutzerfreundliche Software-Anwendung (PRIVACY-AVARE) zu unterstützten. PRIVACY-AVARE soll es den Nutzern ermöglichen, ihre datenschutztechnischen Präferenzen zentral zu bestimmen und global anzuwenden. Dabei sollen die Präferenzen nach dem Festlegen an einer zentralen Stelle auf verschiedene, eigene Endgeräte (Smartphone, Tablet, PC, Fahrzeug, SmartTV, Smart Home, …) übertragen und für verschiedene eigene Dienste (Facebook, XING, …) übernommen und durch technische Maßnahmen (beispielsweise das Unterbinden von Datenzugriffen und Tracking) umgesetzt werden.

Die App PRIVACY-AVARE soll für juristische und technische Laien einfach zu bedienen und rechtskonform einzusetzen sein. Die allgemeinen funktionalen Anforderungen an PRIVACY-AVARE wurden wie folgt definiert:

1. Erfassen des Datenschutzprofils (also der Präferenzen des Nutzers in Bezug auf Datenschutzeinstellungen).
2. Verteilung des Datenschutzprofils.
3. Prüfung auf Verletzungen des Datenschutzprofils.
4. Reduktion der Verletzung des Datenschutzprofils.

Dieser Bericht stellt die Ergebnisse des ersten Meilensteins des AVARE-Projektes vor. Es wird der derzeitige Stand der Wissenschaft und Technik aus den Perspektiven technische Umsetzung, Nutzerfreundlichkeit und rechtliche Implikationen untersucht. Der Fokus der Untersuchungen liegt auf Android, da es mit über 80% weltweit das am weitesten verbreitete Betriebssystem für Smartphones ist (Gartner, 2015). In der Literatur werden bereits einige Risiken und Schwächen des Android Betriebssystems im Hinblick auf Datenschutzeinstellungen beschrieben. Diese werden in Abschnitt 2 gemeinsam mit in der Literatur genannten Lösungsvorschlägen vorgestellt. Der folgende Abschnitt 3 beleuchtet bestehende praktische Lösungsansätze. So wurden im Rahmen des Projekts zunächst Apps zum Schutz der personenbezogenen Daten für Android zusammengetragen und analysiert. Der Begriff „App“ steht dabei für eine Softwareanwendung, die auf sogenannten „Smart Devices“ wie Smartphones, Tablets, Wearables, betrieben werden, aber auch Eingang in Smart-Cars, Smart-TVs, etc. gefunden haben (Kremer et al., 2015, p. 19). Es werden verschiedene Kategorien dieser Apps vorgestellt und die Funktionsweise ausgewählter Apps näher beschrieben, um dann in Abschnitt 3.5 die rechtlichen Impli-

kationen existierender Softwareanwendungen zu betrachten. Zuletzt (Abschnitt 4) schließt ein Ausblick auf die folgende Projektphase (technische und rechtswissenschaftliche Konzeption) diesen Bericht ab.

2 Grundlagen

2.1 Technische Grundlagen

Eine grundlegende Herausforderung für den Schutz personenbezogener Daten auf Smartphones ist die effektive Vergabe von Berechtigungen für Apps: Auf welche Daten und Funktionen darf eine Anwendung zugreifen? Um dies zu kontrollieren implementiert sowohl iOS als auch Android ein Berechtigungssystem. Um auf bestimmte personenbezogene Daten, wie beispielsweise Termine oder Kontakte, zugreifen zu dürfen, muss eine Anwendung diese Berechtigung beantragen. Manche Berechtigungen werden dann vom Betriebssystem automatisch erteilt, andere kann der Nutzer zur Laufzeit (iOS und Android ab Version 6) oder bei Installation (Android) erteilen. Bei Android wird beispielsweise zwischen „normalen“ und „gefährlichen“ Berechtigungen unterschieden. Das Setzen der Zeitzone wäre ein Beispiel für eine normale Berechtigung, wohingegen der Zugriff auf Kontaktdaten als gefährlich eingestuft wird (Google, 2016). Diese vorgegebene Einteilung muss allerdings kritisch betrachtet werden, da beispielsweise auch der Zugriff auf das Internet zu den „normalen“ Berechtigungen zählt. Für den Datenschutz ist diese Berechtigung aber durchaus bedenklich, da über den Internetzugang einmal gesammelte persönliche Daten an Dritte weitergegeben werden können.

Es lässt sich zunächst feststellen, dass viele Apps überprivilegiert sind, d. h. mehr Berechtigungen anfordern als sie tatsächlich benötigen (Felt et al., 2011a). Insbesondere das Berechtigungssystem von Android vor Version 6 wird als wenig effektiv kritisiert, da es zur Folge hat, dass sich viele Nutzer die zu erteilenden Berechtigungen nur flüchtig oder gar nicht durchlesen (Felt et al., 2011b). Darüber hinaus stellen Werbebibliotheken, die oft zur Generierung von Einnahmen in kostenlose Apps integriert werden, ein potenzielles Datenschutzrisiko dar: Sie erhalten dieselben Berechtigungen wie die Apps, in die sie integriert sind, können diese aber beispielsweise dazu verwenden, um detaillierte Nutzerprofile zu erstellen (Stevens et al., 2011). Auch unabhängig von Werbebibliotheken ist es bedenklich, dass Nutzer über IDs (bspw. bei iOS der Unique Device Identifier (UDID)) eindeutig identifizierbar sind -- viele Apps nutzen diese Information und übertragen sie teilweise unverschlüsselt an den jeweiligen Anbieter (Smith, 2010).

Es werden verschiedene Lösungsansätze vorgeschlagen, um den beschriebenen Gefahren zu begegnen. Allgemein kann man zunächst drei Strategien unterscheiden: die Identifikation und Sichtbarmachung von Datenabflüssen (Chun et al., 2010), die Bereitstellung von Fakedaten (Schattendaten) bei Zugriff, sowie die Blockade von Zugriffen (Hornyack et al., 2011). Um bessere Datenschutzentscheidungen durch die Nutzer zu ermöglichen, wird vorgeschlagen, die Anfrage von Berechtigungen zwingend mit Begründungen zu versehen (Lin et al., 2012) und granulare Berechtigungen zu ermöglichen (Nauman et al., 2010). Dem Problem der Werbebibliotheken kann mit einer Trennung der Rechte von Werbebibliotheken und Apps (Liu et al., 2015) begegnet werden.

2.2 Rechtliche Grundlagen

2.2.1 Anwendbarkeit des deutschen Rechtsrahmens

Das deutsche Datenschutzrecht ist in vielen Fällen mit internationalem Bezug nicht einschlägig, womit auch Durchsetzungsdefizite in Drittstaaten einhergehen können. Die Anwendbarkeit deutschen materiellen Datenschutzrechts richtet sich grundsätzlich danach, ob die datenverarbeitende Niederlassung

ihren Sitz in Deutschland, einem anderen EU/EWR-Mitgliedstaat oder einem Drittstaat hat.[1] Ist aufgrund der Belegenheit der maßgeblichen[2] Niederlassung das Recht eines anderen Mitgliedstaates anwendbar, gelten die Grundsätze der RL 95/46/EG[3] in der jeweiligen Umsetzung dieses Mitgliedsstaates. Die Umsetzung der Richtlinie erfolgte jedoch in den Mitgliedstaaten unterschiedlich. Obwohl einige Regelungen einen vergleichbaren Wortlaut verwenden, führte ein unterschiedliches Verständnis der Reichweite und Flexibilität zu uneinheitlicher Anwendung ("Analysis and impact study on the implementation of Directive EC 95/46 in Member States," 2003, p. 9) Mit der kommenden EU-Datenschutzgrundverordnung (DSGVO)[4] wird dieses Problem insoweit behoben, als diese unmittelbar anwendbar ist und damit eine einheitliche Anwendung des materiellen EU-Datenschutzrechts gewährleistet sein dürfte.

Liegt die Niederlassung in einem Drittstaat und erhebt, verarbeitet oder nutzt personenbezogene Daten im Inland ist deutsches Recht anwendbar. Die Übertragung von Daten in Drittstaaten unterliegt nach § 4b BDSG, § 13 Abs. 1 S. 1 TMG weiteren Einschränkungen. Mit Urteil des EuGH vom 06.10.2015 (C-362/14) wurde das „Safe-Harbour" Abkommen, welches einen Datentransfer in die USA ermöglichte, für unwirksam erklärt. Mit dem „Privacy Shield" ist ein neues Abkommen geplant, welches ein angemessenes Schutzniveau sicherstellen soll.

Zur Frage des Datentransfers in Drittstaaten außerhalb von EU/EWR wird es auch künftig nach Art. 44 ff. DSGVO eines Angemessenheitsbeschlusses oder sonstiger geeigneter Garantien bedürfen um sicherzustellen, dass das durch die Verordnung gewährleistete Schutzniveau für natürliche Personen nicht unterlaufen wird. Das kommende „Privacy-Shield"-Abkommen für die Datenübermittlung in die USA wird die vom EuGH gesetzten Standards berücksichtigen müssen (EuGH, Urteil vom 06.10.2015 – C-362/14). Die Notwendigkeit einer angemessenen Durchsetzung von materiellen Rechten in den USA wurde hier adressiert, womit das Durchsetzungsproblem deutlich besser angegangen werden muss, als in der bisherigen Regelung. Darüber hinaus wird das in der DSGVO vorgesehene Marktortprinzip zu einer Ausweitung der Anwendbarkeit auch auf ausländische Unternehmen führen, die betroffenen Personen in der Europäischen Union Waren oder Dienstleistungen anbieten oder das Verhalten betroffener Personen beobachten.

2.2.2 Verantwortliche Stelle

Um das anwendbare Datenschutzrecht zu bestimmen, stellt sich zunächst die Frage nach der verantwortlichen Stelle. Im Rahmen der Nutzung mobiler Apps kommen in der Regel Rechtsbeziehungen zwischen dem jeweiligen Nutzer, dem Store für Apps des jeweiligen Betriebssystems (oder eines Drittanbieters[5]) und dem Anbieter (teilweise gleichzeitig auch Entwickler bzw. Urheber) der jeweiligen App zustande.[6] Im Rahmen der zivilrechtlichen Ausgestaltungen der Vertragsbeziehungen herrscht eine Diskussion darüber, ob der Store-Betreiber lediglich eine Vermittlungsfunktion einnimmt und die Vertragsbeziehung im Rahmen der App-Nutzung primär zwischen Nutzer und App-Anbieter bestehen oder

[1] §§ 1 Abs. 5 S. 1, 3 Abs. 7 BDSG, Art. 2 d), 4 Abs. 1 u. 2 RL 95/46/EG.

[2] Str. zum Fall Facebook: Schleswig-Holsteinisches Oberverwaltungsgericht, Beschluss vom 22. April 2013, Az: 4 MB 11/13 für die Anwendbarkeit irischen Rechts; a.A. KG Berlin, Urteil vom 24.01.2014 – 5 U 42/12.

[3] RICHTLINIE 95/46/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

[4] VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

[5] Aktuell existiert für das Betriebssystem Android neben dem Google Playstore bspw. ein von Amazon betriebener App-Store. Apple IOS hingegen lässt nur den Apple-App-Store zu.

[6] Der Fall eines alternativen Bezugs der App soll hier nicht primär betrachtet werden.

ob vielmehr der Store-Betreiber der eigentliche Vertragspartner des Nutzers ist. (vgl. Baumgartner and Ewald, 2016, p. 3, 6 ; Solmecke et al., 2013, p. 26)(Siehe vereinfachte Darstellung in Abbildung 1)

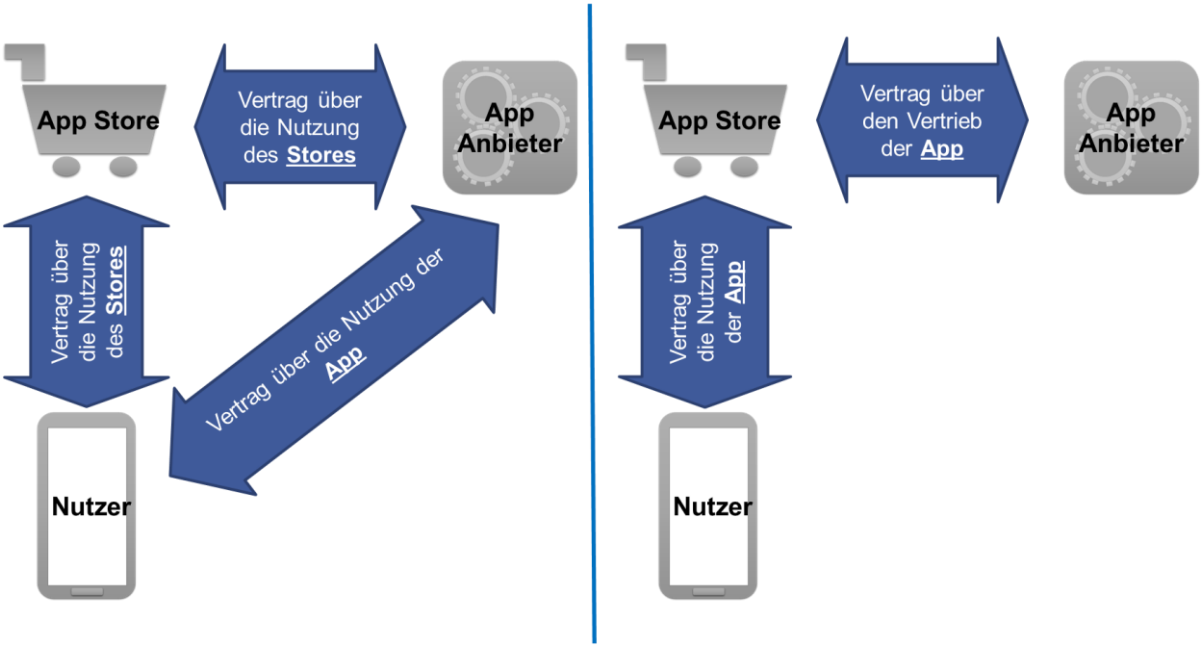

Abbildung 1 Möglichkeiten der Vertragsbeziehungen im Rahmen der Installation und Nutzung einer App

Aus datenschutzrechtlicher Sicht ist für die Frage, welche der beteiligten Rollen für die Einhaltung der Datenschutzbestimmungen gegenüber dem Nutzer verantwortlich ist, entscheidend ob Store-Betreiber und/oder App-Anbieter sowie weitere Akteure (wie bspw. Hersteller Betriebssystem, Hersteller Endgerät, etc.) als „verantwortliche Stelle“ i.S.d. § 3 Abs. 7 BDSG zu qualifizieren sind. Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Werden personenbezogene Daten zur Erbringung des mit der App verbundenen Dienstes an den App-Anbieter übertragen, die dieser selbst verarbeitet/nutzt oder durch Dritte in seinem Namen verarbeiten lässt, so ist dieser in jedem Fall verantwortliche Stelle. Erhält der Store bei Installation der App personenbezogene Daten, ist der Store-Betreiber insoweit stets auch verantwortliche Stelle. In der Regel erfordern App-Stores die Nutzerregistrierung, Hinterlegung von Daten wie Kreditkartennummer oder alternativer Zahlungsmittel und Speichern Informationen zum Kauf- und Nutzungsverhalten, wie eine Liste der heruntergeladenen Apps. Ob der Store-Betreiber darüber hinaus (mit-)verantwortlich für die Datenverwendung im Rahmen der App-Nutzung ist, hängt zunächst davon ab inwieweit die Datenflüsse direkt zwischen Nutzer und App-Anbieter oder über den Store erfolgen (siehe Abbildung 1) und ob eine Datenverarbeitung für eigene Zwecke oder ggf. im Auftrag durch/für den Store erfolgt (vgl. § 11 BDSG).

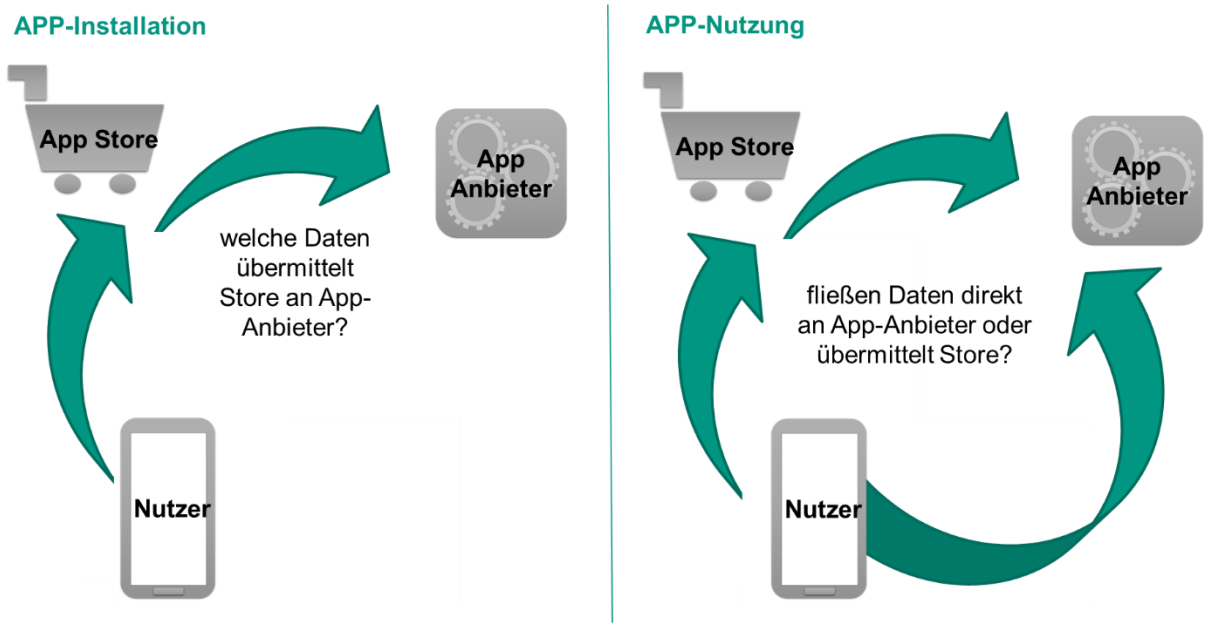

Abbildung 2 Möglichkeiten der Datenflüsse im Rahmen der Installation und Nutzung einer App

Aus Nutzersicht ist die Frage nach der verantwortlichen Stelle insbesondere relevant, um zu wissen gegenüber welcher Stelle datenschutzrechtliche Auskunfts-, Löschungs- und Berichtigungsbegehren geltend gemacht werden können. Darüber hinaus stellt sich die Frage, welche Stelle bei Datenschutzverstößen haftet. Werden personenbezogene Daten an Dritte weitergeleitet (bspw. Werbe- und Marktforschungsunternehmen, Adresshändler etc.) werden diese ebenfalls verantwortliche Stelle, es sei denn es handelt sich um einen Fall der Auftragsdatenverarbeitung. Entscheidend ist, ob diese Stellen Daten zu eigenen Zwecken oder im Auftrag verarbeiten (siehe im Detail: Artikel-29-Datenschutzgruppe, 2013a, pp. 16, 17).

Nach der kommenden DSGVO wird verantwortliche Stelle gemäß Art. 4 (7) EU 2016/679 diejenige Stelle sein, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Nehmen Betriebssystem bzw. Store die Kategorisierung von Datenzugriffsberechtigungen vor, könnte dies als (Mit-)Entscheidung über die Mittel gewertet werden – inwieweit dies auch die Zwecke erfasst, wird zu diskutieren sein (vgl. Artikel-29-Datenschutzgruppe, 2013a).

2.2.3 Legitimation im nationalen Datenschutzrecht

Ist deutsches Datenschutzrecht anwendbar, kann die Datenverwendung durch einen gesetzlichen Erlaubnistatbestand oder eine wirksame Einwilligung des Betroffenen legitimiert werden. Gesetzliche Erlaubnistatbestände für private, nicht-öffentliche Anbieter finden sich u.a. in §§ 28 ff. BDSG, §§ 14, 15 TMG und §§ 91 ff. TMG. Je nach einschlägigem Gesetz bestehen konkrete Anforderungen an die Einholung von Einwilligungen (z.B. Schriftformerfordernis in § 4a Abs. 1 S. 3 BDSG). Für die funktionale Abgrenzung der verschiedenen Anwendungsbereiche von Telemediengesetz (TMG), Telekommunikationsgesetz (TKG) und Bundesdatenschutzgesetz (BDSG) hat sich das sogenannte „Schichtenmodell“ bewährt (Eckhardt, 2015, sec. § 91 TKG Rn. 5; Schaar, 2001, p. 645). Dieses identifiziert die drei folgenden Ebenen:

- Datentransport
- Interaktion zwischen Nutzer und Anbieter
- Inhalt der Kommunikation

Die datenschutzrechtliche Behandlung des Datentransports (Telekommunikation) richtet sich nach dem TKG. Die Interaktion zwischen Nutzer und Anbieter nach dem TMG. Schließlich ist auf das Angebot von solchen Diensten, bei denen der Teledienst lediglich das Übertragungsmedium für andere Leistungen ist – also den Inhalt der Kommunikation –, weiterhin das BDSG anzuwenden (Schaar, 2001, p. 645). Handelt es sich um ein gemischtes Angebot muss aufgrund des unterschiedlichen Schutzzweckes der einzelnen Regelungen das Leistungspaket in die einzelnen Leistungsmerkmale aufgegliedert werden und jeweils gesondert einer Schicht zugeordnet werden (Eckhardt, 2015, sec. § 91 TKG Rn. 5; Kremer, 2012, p. 441)

Die Ausführungen im Folgenden konzentrieren sich auf das TMG, da diese Regelung für die Mehrheit der Apps primär einschlägig sein wird, subsidiär ist stets auf das BDSG zurückzugreifen.[7] Gesetzliche Erlaubnistatbestände für die Erhebung und Verwendung von personenbezogenen Daten zur Bereitstellung von Telemedien finden sich in § 14, 15 TMG für sogenannte „Bestandsdaten“ und „Nutzungs-“ sowie „Abrechnungsdaten“. Personenbezogene Daten, die weder für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind (Bestandsdaten), noch erforderlich sind, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen (Nutzungsdaten), dürfen grundsätzlich nur erhoben und verarbeitet werden, soweit eine wirksame Einwilligung vorliegt. Gemäß § 13 Abs. 2 TMG kann die Einwilligung elektronisch erklärt werden, der Nutzer muss jedoch ausreichend informiert sein und die Einwilligung muss zudem freiwillig erfolgen.

2.2.4 Kollisionen mit Datenschutzprinzipien

Der Schutzkanon des deutschen Datenschutzrechtsrahmens wird durch die bestehenden Schutzprinzipien[8] wie die Gebote der Erforderlichkeit, Zweckbindung, Datensparsamkeit, Datensicherheit und Transparenz dominiert (abhängig von der jeweils einschlägigen einfachrechtlichen Ausprägung) vgl. (Bizer, 2007, p. 350; Wolff et al., 2013, sec. Syst A. Prinzipien). Diese Prinzipien finden sich auch in der kommenden Datenschutzgrundverordnung wieder: Art. 5 nennt hierbei explizit die Grundsätze der Rechtmäßigkeit, Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit sowie Rechenschaftspflicht. Nachfolgend sollen anhand ausgewählter Datenschutzgrundprinzipien regelmäßige Fragestellungen und Kollisionslagen im Zusammenhang mit Smartphone-Apps aufgezeigt werden. Aufgrund der Vielzahl und Eigenart der unterschiedlichsten Apps ist dieser Überblick von generalisierendem Charakter.

2.2.4.1 Konflikt mit den Prinzipien der Erforderlichkeit und Datensparsamkeit

Felt et al. (Felt et al., 2011b) konstatieren, dass gut ein Drittel der untersuchten Smartphone-Apps sich mehr Berechtigungen einräumen lassen, als sie tatsächlich benötigen. Soweit personenbezogene Daten erhoben und verarbeitet werden, die nicht notwendig sind um den Telemediendienst zu erbringen, könnte ein Verstoß gegen den Grundsatz der Erforderlichkeit vorliegen. Dieser Grundsatz ist in §§ 14, 15 TMG durch die Definition der Bestands- und Nutzungsdaten zementiert. Als Begrenzungsfunktion, soll die Datenverwendung auf das für die jeweilige Zweckerreichung

[7] Handelt es sich hingegen um sog. Inhaltsdaten, werden diese überwiegend dem BDSG zugeordnet, wenn bei der Datenverwendung die Telemedien nur als reines Kommunikationsmittel genutzt werden, ohne dass es dabei um eine vertragsgegenständliche Nutzung der Telemedien selbst geht. Die Folge ist das grundsätzliche Schriftformerfordernis bei der Einwilligung nach § 4a Abs. 1 S. 3 BDSG, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Ob diese Ausnahme bei Apps eingreift, ist umstritten. Scheitert eine Legitimation nicht bereits am Formerfordernis, gelten im Rahmen der Einwilligung die gleichen Grundsätze wie nach TMG, d.h. die Einwilligung muss informiert, bestimmt und freiwillig erfolgen.

[8] Auswahl und Anzahl str., vgl. Bizer 2007, p. 350; Wolff in Wolff/Brink, 2013, Syst. A. Prinzipien.

erforderliche Maß beschränkt werden (Zscherpe, 2010, sec. § 14 TMG Rn. 28-38). Auch im Rahmen der Legitimation durch Einwilligung darf die Datenverwendung das zur Erreichung des über die Einwilligung jeweils legitimierten Zwecks erforderliche Maß nicht überschreiten (Bizer, 2007, p. 353).

Im Rahmen der §§ 14, 15 TMG besteht Uneinigkeit darüber, wie eng der Begriff „Erforderlichkeit" auszulegen ist: *Orientiert man sich am Grundsatz der Datenvermeidung und Datensparsamkeit, so dürfen* nur diejenigen personenbezogenen Daten umfasst sein, die zur Gestaltung des konkret betroffenen Telemediendiensteverhältnisses in allen Stadien der Durchführung des Nutzungsverhältnisses *unerlässlich* sind (BT-Drs. 13 / 7385, S. 24; (Müller-Broich, 2012, sec. § 14 Rn. 3; Spindler and Nink, 2015, sec. § 14 TMG Rn. 4). Der Gegenmeinung zufolge entspreche es dem Grundsatz der Privatautonomie dem Diensteanbieter einen gewissen Gestaltungsspielraum zu lassen, so dass die Erlaubnis sich auch auf Daten beziehen soll, die der Sicherung der ordnungsgemäßen Vertrags- bzw. Nutzungsdurchführung vernünftigerweise dienen können aber über den Bereich des zwingend Notwendigen hinausgehen (Plath, 2013, sec. § 14 TMG Rn. 13). Jedenfalls sind personenbezogene Daten, die weder unerlässlich sind noch vernünftigerweise der Abwicklung der Telemediennutzung dienen, nicht erforderlich.

Smith (Smith, 2010) zeigt, dass bei seinen Experimenten 68% der überprüften iOS-Apps Unique Device Identifier (UDID) an den Anbieter der App verschicken. Auch wenn der Anteil inzwischen aufgrund veränderter Apple Guidelines deutlich geringer sein dürfte, können durch UDID betroffene Smartphone und damit auch jeder Nutzer vom App-Anbieter eindeutig identifiziert werden. Werden weitere Daten zur Person kombiniert mit Identifikationsmerkmalen erhoben und gespeichert, besteht die Gefahr der Erstellung von Nutzungsprofilen. Gemäß § 15 Abs. 3 TMG dürfen Nutzungsprofile für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien nur unter Verwendung von Pseudonymen erstellt werden, soweit der Nutzer nicht widerspricht. Laut § 15 Abs. 3 S. 3 TMG dürfen diese Nutzungsprofile nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden. Da bei der Verwendung statischer Pseudonyme eine Identifikation des Betroffenen auch über die Profilbildung meist möglich ist, sollte die Norm restriktiv ausgelegt werden. Eine Profilbildung sollte nur unter temporären Pseudonymen erlaubt sein. Die gewählte Zeitspanne der temporären Pseudonyme sollte so gewählt sein, dass eine Identifikation des Betroffenen unter verhältnismäßigem Aufwand nicht möglich ist. Daher sollte die Profilbildung nicht mithilfe der UDID, IMEI[9], IMSI[10] oder Mobilfunknummer erfolgen, da über diese eine eindeutige Identifikation mit verhältnismäßigen Mitteln wahrscheinlich erscheint. Darüber hinaus wird bemängelt, dass bei vielen Apps der gesonderte Hinweis auf das Widerspruchsrecht nach § 15 Abs. 3 S. 2 TMG fehle (Bodden et al., 2013, p. 724). Dies führt in derartigen Fällen zur Unzulässigkeit der Profilbildung.

Überdies verpflichtet § 13 Abs. 6 TMG Diensteanbieter die Nutzung ihrer Telemediendienste und deren Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Aus rechtlicher Sicht stellt sich in diesem Zusammenhang die Frage, wie Nutzer mit Angeboten umgehen dürfen, die entgegen § 13 Abs. 6 TMG die Angabe des Klarnamens oder weiterer persönlicher Daten bspw. in ihren AGB verlangen. Laut dem Norton Cybercrime Report hat etwa die Hälfte der Befragten bereits falsche Angaben im Internet gemacht oder sogar falsche Identitäten verwendet (Norton, 2011). Ob eine solche „digitale Notlüge" ohne Vertragsverletzung rechtlich zulässig ist, wurde bisher rechtlich noch nicht umfassend erörtert (Karger, 2010). Schnabel/Freund beschäftigen sich in ih-

[9] International Mobile Equipment Identity: eine eindeutige 15-stellige Seriennummer, anhand derer jedes GSM- oder UMTS-Endgerät weltweit eindeutig identifiziert werden kann.
[10] International Mobile Subscriber Identity

rem Aufsatz daher mit der Frage, wann eine falsche Angabe über § 13 Abs. 6 TMG legitimiert ist (Schnabel and Freund, 2010, p. 718). Dabei ist zunächst zu untersuchen, inwieweit die anonyme/pseudonyme Dienstnutzung gegenüber dem Dienstanbieter, oder lediglich gegenüber Drittnutzern ermöglicht werden muss. Im Ergebnis ist ihnen zuzustimmen, dass aus systematischen Erwägungen sowie als effektive bereits bei der Datenentstehung ansetzende Konkretisierung des Gebots der Datensparsamkeit auch die Anonymität / Pseudonymität gegenüber dem Dienstanbieter ermöglicht werden muss – soweit möglich und zumutbar (a.A. OLG Düsseldorf, Urteil vom 07. Juni 2006 – I-15 U 21/06 noch zu § 4 Abs. 6 TDDSG wonach lediglich die Inanspruchnahme und Bezahlung erfasst sei – nicht jedoch der Vertrag mit dem Anbieter). Dieser Unterscheidung zwischen Nutzung und Bezahlung des Telemediendienstes einerseits und Vertragsschluss andererseits folgen auch Spindler / Nink, die die Norm für die Nutzung des Telemediendienstes aber sowohl gegenüber anderen Nutzern als auch gegenüber dem Anbieter des Telemediendienstes anwenden wollen (Spindler and Nink, 2015, sec. § 13 TMG Rn. 22). Dies würde dann jedoch nur noch zu einer pseudonymen Nutzung von Telemedien führen, wenn der Anbieter des Dienstes die Person über den Vertrag eindeutig zuordnen kann. Nach der relativen Theorie zum Personenbezug (siehe zur Erklärung: Dammann, 2014, sec. § 3 Rn. 25) kann diese pseudonyme Nutzung zur Annahme von Anonymität gegenüber anderen Nutzern führen.[11] Nach der objektiven Theorie zum Personenbezug (siehe Schlussanträge des Generalanwalts vom 12. Mai 2016 in der Rechtssache C-582/14)[12] würde im Fall der Zuordenbarkeit durch den Anbieter eine anonyme Nutzung (im Rechtssinne) im Prinzip ausscheiden (es sei denn der Zugang zu den Zuordnungsdaten ist nicht realisierbar). In diesem Fall wäre der Wortlaut als eindeutiges Indiz zu werten, dass die Norm sowohl die Beziehung zu anderen Nutzern als auch zum Anbieter selbst erfasst. Zudem stellt sich die Frage zur Abgrenzung gegenüber § 13 Abs. 4 Nr. 3 TMG, welcher dem Schutz der Vertraulichkeit der Nutzungen gegenüber Dritten dient.

Im Gegensatz zu den Legitimationsgrundlagen §§ 14 Abs. 1, 15 Abs. 1 TMG macht § 13 Abs. 6 TMG eine anonyme Nutzung nicht von der „Erforderlichkeit", sondern „Zumutbarkeit" abhängig: sind die Daten für die Diensterbringung in der vom Anbieter vorgesehenen Art und Ausgestaltung des Dienstes erforderlich, kann sich die Frage der Zumutbarkeit im Verhältnis zum Anbieter nur gegenüber dem gesamten Geschäftsmodell stellen. Ist ein auf anonymer Datenverwendung beruhendes Geschäftsmodell nicht zumutbar, können erforderliche Daten nach §§ 14 Abs. 1, 15 Abs. 1 TMG erhoben werden. Die Norm kann darüber hinaus im Rahmen der Legitimation durch Einwilligung Bedeutung erlangen: sollen mittels einer Einwilligung über die Diensterbringung hinausgehende Daten erhoben werden und ist die anonyme Dienstbereitstellung dem Anbieter zumutbar, müsste dem Nutzer eine solche Möglichkeit angeboten werden.

Zum Grundsatz der Datensparsamkeit wird jedoch konstatiert, dass ein Verstoß sanktionslos bleibt (Forum Privatheit, 2014, p. 6; Spindler and Nink, 2015, sec. § 13 TMG Rn. 20). Ein Verstoß gegen § 13 Abs. 6 TMG ist nicht im Bußgeldkatalog des § 16 TMG enthalten. Schnabel/Freund hingegen gehen davon aus, das AGB-Vorgaben zur Angabe personenbezogener Daten bei Verstoß gegen § 13 Abs. 6

[11] Nach der relativen Theorie liegt ein personenbezogenes Datum lediglich dann vor, wenn die konkret verarbeitende Stelle mit vertretbarem Aufwand eine Identifikation der natürlichen Person vornehmen kann, sodass ein Datum für eine Stelle personenbezogen und für eine andere Stelle anonym sein kann (es sei denn es liegt ein Zusammenwirken der Stellen vor)

[12] Nach der objektiven Theorie ist Personenbezug anzunehmen, wenn irgendjemand die Zuordnung des Datums zu einer Person vornehmen kann (unabhängig davon, ob die konkret verantwortliche Stelle rechtmäßig an diese Information gelangen kann)

TMG nach § 307 Abs. 2 Nr. 1 BGB unwirksam sind. Die Annahme einer falschen Identität könnte demnach vom Anbieter (jedenfalls) nicht unter Verweis auf seine AGB-Bestimmungen geahndet werden (Schnabel and Freund, 2010, p. 720). Grundsätzlich stellt sich jedoch zum einen die Frage, wann Zumutbarkeit angenommen werden kann und ob auch weitere Gründe die Nutzung alternativer Identitäten rechtlich ausschließen.

2.2.4.1.1 Spannungsverhältnis der Datensparsamkeit zur Rechtsverfolgung

Die Pflicht zur Ermöglichung einer anonymen / pseudonymen Nutzbarkeit digitaler Angebote kann im Interessenkonflikt zur Verfolgbarkeit von Rechtsverstößen im Internet, wie bspw. der unzulässigen Verbreitung urheberrechtlich geschützter Film- und Musikwerke, stehen. So entschied das OLG Hamburg, dass sich Betreiber von Sharehosting-Diensten nicht auf § 13 Abs. 6 TMG berufen könnten, wenn damit erforderliche Prüf- und Kontrollmaßnamen unterblieben und so den Urheberrechtsverletzungen dank der Anonymität der Nutzer Vorschub geleistet würde (Hanseatisches Oberlandesgericht Hamburg, Urteil vom 02. Juli 2008 – 5 U 73/07). Zu den vom Gericht verlangten Identifikationsmaßnahmen (Nutzerkonto, Verbot dynamischer IP-Adressen oder Proxy-Server) räumt es zwar selbst ein: „dass derartige Maßnahmen keinen vollständigen Schutz bieten, versteht sich von selbst." Gleichwohl geht das Gericht davon aus, dass die Maßnahmen „Rechtsverletzungen nachhaltig entgegenwirken" (Hanseatisches Oberlandesgericht Hamburg, Urteil vom 02. Juli 2008 – 5 U 73/07). Demgegenüber vertreten OLG Köln und OLG Düsseldorf, dass Diensteanbieter in vergleichbaren Fällen nicht für urheberrechtsverletzende Inhalte auf den von Nutzern zum Download angebotenen Dateien haften und eine Nutzeridentifizierung erforderliche Prüfmaßnahmen nicht zumutbar ist, wenn tatsächlich keine effektiven Möglichkeiten der Vorbeugung, Verhinderung und nachträglichen Beseitigung inklusive einer Wiederholung der Verbreitung von urheberrechtlich geschütztem Material bestehen (OLG Köln, Urteil vom 21. September 2007 – 6 U 86/07; OLG Düsseldorf, Urteil vom 27. April 2010 – I-20 U 166/09; OLG Düsseldorf, Urteil vom 21. Dezember 2010 – I-20 U 59/10). Dementsprechend wurde von den Gerichten nicht verlangt, dass der Anbieter sein auf der anonymen Nutzbarkeit beruhendes Geschäftsmodell aufgibt. Trotz dieser Argumente hat das OLG Hamburg seine Rechtsprechung im Fall Rapidshare II bestätigt (Hanseatisches Oberlandesgericht Hamburg, Urteil vom 30. September 2009 – 5 U 111/08). Das Gericht folgt der grundsätzlichen Annahme des BGH, Anonymität im Netz führe zu einer herabgesetzten Hemmschwelle (BGH, Urteil vom 12. Juli 2007 – I ZR 18/04 –, BGHZ 173, 188-210, Rn. 26). Entscheidendes Kriterium für die Unlauterkeit des Geschäftsmodells dürfte in diesem Fall aber weniger die Tatsache der Anonymität sein, sondern dass die Plattform regelmäßig im Millionenwert für den kostenlosen Austausch lizenzpflichtiger Film- und Musikwerke sowie Computerprogramme genutzt wurde. Die Unzumutbarkeit der anonymen/pseudonymen Bereitstellung von Telemedien dürfte hingegen nicht anzunehmen sein, wenn Rechtsverstöße nur vereinzelt oder beiläufig von Nutzern zu befürchten sind bzw. nicht naheliegend erscheinen. So entschied ebenfalls das OLG Hamburg im Fall eines einmaligen Urheberrechtsverstoßes durch einen Nutzer: „Denn auch anonym oder unter Pseudonym nutzbare Internetforen stellen ein grundsätzlich zulässiges und auch übliches Geschäftsmodell im Internet dar und stehen unter dem Schutz der Meinungsäußerungs- und Pressefreiheit. Wie die Regelung des § 13 Abs. 6 TMG zeigt, ist die anonyme Nutzung des Internets sogar ausdrücklich geschützt, …" (Hanseatisches Oberlandesgericht Hamburg, Urteil vom 04. Februar 2009 – 5 U 180/07)

Die Rechtsprechung des OLG Hamburg im Fall Rapidshare wurde in der Literatur kontrovers diskutiert. Abgelehnt wird zum einen die Erhebung und Speicherung von Nutzungsdaten „auf Vorrat" für den Fall der Weitergabe an Dritte zur Rechtsverfolgung, da die teils von der Rechtsprechung herangezogene Legitimationsgrundlage (§ 101 Abs. 9 UrhG) dieser Weitergabe nicht einschlägig sei (Barnitzke, 2010, p. 484). Die Forderung zur Angabe von identifizierenden Daten wird darüber hinaus wegen der leichten

Umgehungsmöglichkeit als ungeeignetes Mittel abgelehnt und zum anderen wegen der fehlenden Erforderlichkeit für die Diensterbringung selbst (in diesem Fall zur Verfügung stellen von Speicherplatz) als datenschutzwidrig eingestuft (Breyer, 2009, p. 16). Gabriel und Albrecht (Gabriel and Albrecht, 2010, p. 394) gehen dagegen davon aus, dass zur Abwendung der Störerhaftung eine Rechtspflicht erwachse, IP-Adressen zu speichern bzw. eine Identifikationspflicht einzuführen, um künftige Verletzungen der gleichen Nutzer zu unterbinden – ohne auf die datenschutzrechtliche Legitimationsbedürftigkeit oder Geeignetheit der vorgeschlagenen Maßnahmen überhaupt einzugehen. Ebenso verlangt Nordemann Vorsorgemaßnahmen gegen Rechtsverletzungen durch Plattform-Nutzer mittels Nutzeridentifikation, Einrichtung eines Lösch-Interface für Rechteinhaber oder Aufgabe des Geschäftsmodells (Nordemann, 2010, p. 605).

Zur Beantwortung der Frage der Zumutbarkeit in Bezug auf Schutzmaßnahmen für Rechteinhaber (bis hin zur Einstellung der Tätigkeit) auf der einen Seite und der anonymen Nutzbarkeit auf der anderen Seite bedarf es neben der eingehenden Prüfung der Geeignetheit geforderter Identifikationsmaßnahmen auch einer Abwägung der Grundrechte des Plattformnutzers, des Plattformbetreibers und des Rechteinhabers. So stehen im widerstreitenden Konflikt das Recht auf informationelle Selbstbestimmung und der Meinungs- und Informationsfreiheit des Nutzers, die Berufsfreiheit des Plattformbetreibers sowie das Recht auf Eigentum des Rechteinhabers. Bestehen aber bereits keinerlei geeignete Vorsorgemaßnahmen (unabhängig von der Frage einer rechtlichen Verpflichtung Vorsorge zu betreiben) erscheint diese Abwägung obsolet.

Ob man die Rapidshare-Rechtsprechung des OLG Hamburg zur Zumutbarkeit i.S.d. § 13 Abs. 6 TMG auf sämtliche Fälle potentiell erforderlicher Rechtsverfolgungsbegehren Dritter übertragen kann ist daher eher zweifelhaft. Grundsätzlich ermöglicht auch die Anonymität im Netz die Begehung von Straftaten wie Beleidigungen. Ein Forumsbetreiber, soziales Netzwerk oder Betreiber einer Bewertungsplattform ist laut aktueller Rechtsprechung aber nicht verpflichtet, sein Angebot auf die nicht-anonyme Nutzung zu beschränken. Aus grundrechtlicher Sicht hatte der BGH den Konflikt neben dem Recht auf informationelle Selbstbestimmung zwischen dem allgemeinen Persönlichkeitsrecht der diffamierten Personen und dem Recht auf freie Meinungsäußerung nach Art. 5 Abs. 1 S. 1 GG zu entscheiden (vgl. BGH, Urteil vom 23.06.2009, Az. VI ZR 196/08; vgl. auch OLG Düsseldorf, Urteil vom 07. Juni 2006 – I-15 U 21/06, 15 U 21/06; LG München I, Urteil vom 03. Juli 2013 – 25 O 23782/12).

2.2.4.1.2 Selbstdatenschutz im Konflikt mit der Rechtsordnung

Wird die Preisgabe identifizierender Merkmale verlangt und gibt der Nutzer nicht die korrekten Daten ein, müssen stets rechtliche Implikationen bedacht werden. Bezüglich der Grenzen des Selbstdatenschutzes ist auch auf die folgenden rechtlichen Diskussionen hinzuweisen.

2.2.4.1.2.1 Strafbarkeit erfundener Nutzer-Accounts?

Das KG Berlin entschied, dass die Einrichtung eines Mitgliedskontos unter falschen Personalien bei der Auktionsplattform eBay im Internet den Tatbestand des § 269 Abs. 1 StGB erfüllen kann (KG Berlin, Beschluss vom 22. Juli 2009 – (4) 1 Ss 181/09 (130/09)). Es handele es sich grundsätzlich um die Speicherung beweiserheblicher Daten derart, dass bei ihrer Wahrnehmung eine unechte Urkunde im Sinne des § 267 Abs. 1 StGB vorliegen würde. Dagegen geht das OLG Hamm davon aus, in der Anlegung eines Accounts bei eBay liege keine Speicherung beweiserheblicher Daten, weil eine rechtlich relevante Gedankenerklärung fehle, sondern es sich lediglich um einen Vorgang ohne jeden nach außen hinwirkenden Erklärungscharakter handele (vgl. OLG Hamm, Beschluss vom 18. November 2008 – 5 Ss 347/08).

Grundsätzlich ist bei rechtsrelevantem Handeln zu unterscheiden, ob es sich um eine Namens- oder Identitätstäuschung handelt. Im Falle einer bloßen Namenstäuschung kann die Täuschungsabsicht fehlen, wenn sich der Aussteller ungeachtet der falschen Namensnennung an seiner im Rechtsverkehr wirkenden Erklärung festhalten lassen will (vgl. BGH, Beschluss v. 21.03.1985, 1 StR 520/84; OLG Oldenburg, Beschluss vom 18. April 2013 – 1 Ws 88/13). Dies gilt insbesondere, wenn sein Gegenüber kein schutzwürdiges Interesse an der korrekten Namensangabe hat. Maßgeblich für die Frage, ob eine bloße Namens- oder eine Identitätstäuschung vorliegt, ist das – für den Täter erkennbare – Interesse des Gegenübers im Rechtsverkehr an seiner Identität (KG Berlin, Beschluss vom 22. Juli 2009 – (4) 1 Ss 181/09 (130/09) –, Rn. 41). Bei der Einrichtung eines Nutzerkontos bleibt jedoch zu prüfen, welche Angaben tatsächlich erforderlich sind und inwieweit eine Nutzung unter Pseudonym gegenüber anderen Nutzern möglich und zumutbar ist. Der dem KG Berlin vorliegende Fall ist daher von der Einrichtung eines kostenlosen E-Mail-Accounts bei einem sog. Freemailer zu unterscheiden. Mangels einer nach außen wirkenden Erklärung bei der Einrichtung des Kontos – abzugrenzen von einer (späteren) missbräuchlichen Nutzung des Accounts – wird vertreten, dass es sich um eine straffreie Vorbereitungshandlung handele (vgl. KG Berlin, Beschluss vom 22. Juli 2009 – (4) 1 Ss 181/09 (130/09) –, Rn. 35). Um tatbestandsmäßig „beweiserhebliche Daten“ zu fälschen, müssen die Daten sowohl in objektiver als auch subjektiver Hinsicht geeignet und dazu bestimmt sein, als Beweis für rechtlich relevante Handlungen zu dienen. Liegt die Verwendungsabsicht des Ausstellers nicht in der Verwendung im Rechtsverkehr als Beweis bestimmter Rechtsverhältnisse, sondern lediglich darin seine Anonymität zu wahren, fehlt die Beweisbestimmung (Buggisch, 2004, p. 3520). Bei einem Freemailer wird aufgrund der Unentgeltlichkeit des Free-Mail-Accounts davon ausgegangen, dass es diesem gleichgültig ist, wer unter welchen Personalien ein solches E-Mail-Konto einrichtet.

Werden im Rahmen von Selbstdatenschutzlösungen falsche Daten übermittelt, sollte im Einzelfall geprüft werden, inwieweit die objektiven und subjektiven Tatbestandsmerkmale des § 269 Abs. 1 StGB erfüllt sein können. Bei einigen Datenkategorien, wie bspw. GPS-, Kontakt-, oder Sensordaten, dürfte jedoch bereits in dem anzustellenden Vergleich mit einer unechten oder verfälschten Urkunde die für die Urkundenfälschung maßgebliche Täuschung über den Aussteller fehlen, da über diese Daten (allein) kein Aussteller erkennbar sein dürfte. Wesentliches Merkmal der Urkundenfälschung ist, dass über die wahre Identität des Ausstellers getäuscht wird (Buggisch, 2004, p. 3521). Um überhaupt in den Anwendungsbereich von § 269 StGB zu fallen, muss es sich um die Falschangabe von Identifizierungsmerkmalen handeln.

2.2.4.1.2.2 Impressumspflicht für private Nutzerseiten sozialer Medien?

Richter (Richter, 2014, p. 517) befasst sich mit dem Widerspruch der Ermöglichung der anonymen Nutzung sozialer Netzwerke nach § 13 Abs. 6 TMG und der Ansicht, die Impressumspflicht nach § 55 Abs. 1 RStV würde auch für private Profile in sozialen Netzwerken gelten. Trotz der eindeutigen Ausnahme für ausschließlich persönliche oder familiäre Zwecke kommt Rockstroh zu dem Ergebnis, dass auch sämtliche private Profilseiten in sozialen Netzwerken der Impressumspflicht nach § 55 Abs. 1 RStV unterfallen sollen (Rockstroh, 2013, p. 630). Dies hätte zur Folge, dass jeder auch private Nutzer Namen und Anschrift leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten hätten. Seiner Ansicht nach lägen nicht ausschließlich familiäre oder persönliche Zwecke vor, wenn Sinn und Zweck des Betriebs einer Facebook-Seite darin lägen, mit Menschen in Kontakt zu treten, mit denen man nicht persönlich verbunden sei. Die Facebook-Seite diene dementsprechend keinen privaten Zwecken, sondern der Präsentation einer öffentlichen Person. Dies mag für Unternehmen oder Personen des öffentlichen Lebens aber wohl kaum für die Durchschnittsnutzer zutreffen. Insoweit dürfte § 13 Abs. 6

TMG grundsätzlich auch auf soziale Netzwerke anwendbar sein. Nach der Anordnung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) gegenüber Facebook die Klarnamenpflicht aufzugeben (siehe Pressemitteilung vom 17.12.2012, abrufbar unter https://www.datenschutzzentrum.de/presse/20121217-facebook-klarnamen.htm), ist die gerichtliche Entscheidung zur Anwendbarkeit von § 13 Abs. 6 TMG auf Facebook bisher an der Nichtanwendbarkeit des deutschen Datenschutzrechts gescheitert (OVG Schleswig Beschl. v. 22.04.2013 – 4 MB 11/13 a.A. KG Berlin, Urt. v. 24.01.2014 – 5 U 42/12).

2.2.4.1.2.3 Zusammenfassung

Diese genannten Beispiele zeigen, dass die Durchsetzung des Rechts auf informationelle Selbstbestimmung grundsätzlich mit entgegenstehenden Grundrechtspositionen der betroffenen Gegenpartei (i.d.R. der verantwortlichen Stelle) oder auch Dritter (ggf. Rechteinhaber bei Verletzungshandlungen durch Telemediennutzer) abzuwägen sind. Die Verwendung falscher Daten kann die Anonymität der Nutzer digitaler Medien gewährleisten bzw. eine Teilnahme an digitalen Kommunikationsprozessen unter Pseudonym ermöglichen. Zuvor sollten jedoch rechtsgebietsübergreifend Schranken identifiziert und geprüft werden, welche ein solches Vorgehen ausschließen. Das Spannungsverhältnis der Datenschutzrechte zu widerstreitenden Offenlegungsinteressen im Kontext der Nutzung mobiler Apps wird im weiteren Projektverlauf einen Schwerpunkt der rechtlichen Untersuchungen darstellen.

2.2.4.2 Zweckbindung

Der Grundsatz der Erforderlichkeit wird flankiert durch den Grundsatz der Zweckbindung, wonach grundsätzlich personenbezogene Daten nur für einen vorab festgelegten Zweck verarbeitet werden dürfen, es sei denn es liegt ein Fall einer zulässigen Zweckänderung vor. (vgl. Art. 8 Abs. 2 EU-Grundrechte-Charta; Art. 6 Abs. 1 (b) RL 95/46/EG; Art. 5 Abs. 1 (b) EU 2016/679 (DSGVO); § 12 Abs. 2 TMG) Kritisch im Zusammenhang mit der Zweckbindung ist die Zusammenführung von Daten aus unterschiedlichen Kontexten zu bewerten, denn die Zweckbestimmung dient auch dazu dem Betroffenen einen Verwendungskontext nachvollziehbar transparent zu machen (Artikel-29-Datenschutzgruppe, 2013a, p. 22, 2013b, p. 4). Die technisch-organisatorische Maßnahme der Datentrennung i.S.d. Nr. 8 Anlage zu § 9 S. 1 BDSG gebietet – soweit der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht – zu unterschiedlichen Zwecken erhobene Daten nicht zusammenzuführen. Besonders kritisch ist daher die Wiederzuordnung gesammelter technischer Daten durch Webtracking (siehe hierzu Abschnitt 2.2.5). Dienste wie z.B. Google-Analytics oder Google-Adsense versuchen auf Basis gesammelter Daten gezielt personalisierte Werbung und Empfehlungen anwendungs- bzw. webseitenübergreifend anzuzeigen. Hierfür müssen i.d.R. Profile der Nutzer über Interessen und Vorlieben angelegt und zentral verwaltet werden. Durch den Einsatz solcher Werbedienste kann ein Netz an Anwendungen und Webseiten entstehen, über welche ein Nutzer verfolgt werden kann. Daraus werden Daten extrahiert, die wertvoll für die Anbieter von Webinhalten sind. Sowohl der materielle Wert der Daten für den Verwerter als auch die persönlichkeitsrechtliche Bedeutung für den Betroffenen variieren mit dem jeweiligen Kontext (Beisenherz and Tinnefeld, 2011, p. 111). Unter dem Stichwort „Big Data“ sollen Mehrwerte gerade durch die Zusammenführung von personenbezogenen Daten über die Erhebungskontexte hinaus generiert werden (Roßnagel, 2013; Weichert, 2013). Datenschutzrechtlich brisant ist zum einen, dass dadurch wesentlich umfangreichere Persönlichkeitsbilder entstehen können. Zum anderen gewähren gesetzliche Erlaubnistatbestände die Datenverwendung

nur zu einem bestimmten Zweck (vgl. §§ 14, 15 TMG[13]) oder die Legitimation unterliegt einer Interessenabwägung, deren Ausgang regelmäßig vom verfolgten Zweck abhängig ist (vgl. § 28 BDSG). Im Falle einer Einwilligung ist keine wirksame Selbstbestimmung gegeben, wenn diese nicht auf einen bestimmten Verwendungskontext und damit bestimmten Verwendungszweck beschränkt ist (Beisenherz and Tinnefeld, 2011, p. 111).

Dementsprechend handeln Apps datenschutzwidrig, wenn die verfolgten Zwecke nicht vorab (dokumentiert bspw. in Textform) vor der ersten Datenerhebung festgelegt werden oder im Falle der erfolgten Festlegung die anschließende Datenverwendung diese festgelegte Zweckverfolgung überschreitet (es sei denn es liegt ein gesetzlicher Erlaubnistatbestand zu einer Zweckänderung vor.) Entscheidend für den ersten Schritt der Zweckfestlegung ist die Frage, wie konkret Zwecke benannt werden müssen. Hierzu hat die Artikel-29-Datenschutzgruppe auf Grundlage von Art. 5 Abs. 1 Buchst. (b) RL 95/46/EG eine Stellungnahme veröffentlicht (Artikel-29-Datenschutzgruppe, 2013b). Eine gesetzliche Erlaubnis der Verwendung von Bestands- oder Nutzungsdaten zu anderen Zwecken als der Bereitstellung von Telemedien sowie der Abrechnung finden sich bspw. in:

- § 14 Abs. 2 / § 15 Abs. 5 S. 4 TMG (Zwecke der Strafverfolgung, zur Gefahrenabwehr oder zur Durchsetzung der Rechte am geistigen Eigentum)
- § 15 Abs. 3 TMG (Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien)
- § 15 Abs. 4 S. 2 TMG (Erfüllung bestehender gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsfristen)
- § 15 Abs. 8 TMG (Zwecke der Rechtsverfolgung)

Weitere Zweckänderungen gestattende Erlaubnisnormen außerhalb des TMG, die sich auf Telemedien beziehen, existieren derzeit nicht (Moos, 2010, sec. § 12 TMG Rn. 20; Schreibauer, 2014, sec. § 12 TMG Rn. 13; Spindler and Nink, 2015, sec. § 12 Rn. 7)

Um zweckentfremdende Datenverwendung zu verhindern, wird Nutzern u.a. empfohlen, für jeden Zweck ein separates Pseudonym zu verwenden (Forum Privatheit, 2014, p. 6). Ob dies vor dem Hintergrund effektiver Webtracking-Technologien (siehe Abschnitt 2.2.5) effektiven Selbstdatenschutz gewährleistet, ist durchaus fraglich. Daher dürfte es technischer Selbstdatenschutz-Lösungen bedürfen.

2.2.4.3 Transparenz und Einwilligung

Nutzer von mobilen Anwendungen, deren personenbezogene Daten im Zuge dieser Anwendung preisgegeben werden, müssen durch die für die Datenerhebung und -verwendung verantwortliche Stelle in die Lage versetzt werden, die Datenübermittlung nachzuvollziehen (Düsseldorfer Kreis, 2011, p. 1). Dies bezieht sich nicht nur auf die Auswahl der übertragenden Daten, sondern auch auf die Verwendungszwecke, Art und Umfang der Erhebung und Verwendung, Übermittlung der Daten in Drittstaaten außerhalb der EU/EWR, Identität der verantwortlichen Stelle sowie weiterer Empfänger bzw. Kategorien der Empfänger dieser Daten (vgl. § 13 Abs. 1 TMG, § 4 Abs. 2 BDSG). Soll die Datenverwendung durch eine wirksame Einwilligung legitimiert werden, muss diese ausreichend informiert, freiwillig und ausreichend bestimmt erfolgen (Simitis, 2014, sec. § 4a Rn. 62ff.).

[13] Inwieweit die Einschränkungen des § 15 Abs. 1 TMG auf Zwecke der (aktuellen) Nutzung und Abrechnung mit der RL 95/46/ EG vereinbar ist, wird im anhängigen Verfahren Rs. C-582/14 durch den EuGH entschieden.

2.2.4.3.1 Informiertheit

Um die erforderlichen Informationspflichten zu erfüllen, sollen in der Regel Datenschutzerklärungen dienen, die dann auch einer Einwilligung zugrunde gelegt werden können. Jedoch ergab eine Studie aus dem Jahr 2012, dass lediglich 61,3% der 150 beliebtesten Apps überhaupt eine Datenschutzerklärung hatten (FUTURE OF PRIVACY FORUM, 2012). Diese Datenschutzerklärungen schaffen jedoch mangels Wahrnehmung durch die Betroffenen kaum die erforderliche Transparenz (Hornung and Goeble, 2015, p. 270; Jöns, 2015; Schwartmann and Hentsch, 2015, p. 228). Eine europäische Studie zeigte, dass lediglich 12% der befragten Europäer Datenschutzerklärungen tatsächlich lesen (Vodafone Institute for Society and Communication, 2016). Bemängelt wird vor allem, dass die Erklärungen oft eher darauf zugeschnitten sind, als Grundlage einer rechtlichen Absicherung für die verantwortliche Stelle zu dienen, als eine verständliche Informationsquelle für den Nutzer zu gewährleisten (sogar von bewusster Desinformation spricht: Jöns, 2016, p. 54, 2015). So wird vielfach die Länge und Komplexität, wie bspw. die gewählte „juristische" Sprache bemängelt (DIVSI, 2014, p. 17). Der Umfang der Erklärungen erschwert es zudem häufig die Kernaussagen in verhältnismäßigem Zeitaufwand zu erfassen (Fetzer, 2015, p. 778). Laut einer Studie liegt das durchschnittliche Wissensniveau der Befragten bezüglich der umfassenden Kenntnis der über sie erhobenen personenbezogenen Daten bei lediglich 23% (Vodafone Institute for Society and Communication, 2016, p. 13). Ebenso werden Auskunftsverlangen nicht in allen Fällen umfassend beantwortet (IRISS, 2015).

Soll die datenschutzrechtliche Einwilligung durch die Betätigung des „Installieren"-Buttons (oder einer ähnlichen Vorrichtung) erteilt werden, so dürfte die räumlich getrennte Verlinkung der Datenschutzerklärung (insbesondere, wenn diese erst durch längeres Scrollen auffindbar wird) für eine wirksame Einwilligung nicht ausreichen (vgl. LG Berlin, Urteil vom 28. Oktober 2014 – 16 O 60/13.) Dem Nutzer muss vielmehr die Tragweite seiner Entscheidung bewusst gemacht werden, insbesondere welchem Zweck die Datenverwendung dient und welche Reichweite die Einwilligung hat (z.B. Datenübermittlung an Dritte). Die erforderliche Information wird i.d.R. auch nicht über die Zustimmung zu den Berechtigungsanfragen vermittelt, da hier gerade der Grund der Berechtigungsanfrage nicht angegeben wird – oder ob eine Weitergabe von Daten an Dritte beabsichtigt ist.

Die kommende Datenschutzgrundverordnung enthält erste Ansätze, die mehr Transparenz und Wahlfreiheit der Betroffenen versprechen (je nach praktischer Umsetzung und Interpretation der Regelungen). Durch die Möglichkeit standardisierte Bildsymbole in Kombination mit Datenschutzerklärungen zu verwenden, erfolgt zum einen die vereinfachende Wahrnehmbarkeit in einer schnelllebigen Zeit, zum anderen die Standardisierung von Datenschutzerklärungen. Dies stärkt die Vorhersehbarkeit und Vergleichbarkeit von Angeboten. Zudem wird die Maschinenlesbarkeit elektronischer Symbole den Datenschutz insoweit stärken, indem Nutzer ihre Datenschutzpräferenzeinstellungen durch Selbstdatenschutz-Apps für sämtliche Anwendungen vornehmen können und dabei auch die Datenschutzerklärungen (bspw. Zweckangabe) berücksichtigen können. Die Regelung setzt jedoch auf den freiwilligen Einsatz dieser Innovationen.

2.2.4.3.2 Freiwilligkeit

Zudem wird kritisiert, dass die Installation von Apps häufig von der Einwilligung in umfassende Zugriffsrechte nach einer Art „Alles-oder-nichts-Prinzip" abhängig gemacht wird (Brummund, 2014, p. 539). Die Kopplung des Angebots an die Abgabe einer Einwilligungserklärung lässt Nutzern bei Machtasymmetrien wie bei Monopolstellungen, informationellen Ungleichgewichten, aber auch im Bereich der lebensnotwendigen Daseinsvorsorge kaum Spielraum (Kamp and Rost, 2013, p. 82). Nutzern verbleibt bei digitalen Plattformen zwar theoretisch die Wahl auf das Angebot zu verzichten, Netzwerkeffekte

führen jedoch häufig dazu, dass zur Teilnahme am sozialen Leben der Beitritt zur Plattform mit den meisten Nutzern alternativlos ist und damit kein ernst zu nehmender Verhandlungsspielraum besteht (Schwartmann and Hentsch, 2015, p. 228). Zweifel an der Freiwilligkeit der Einwilligung entstehen daher auch dann, wenn über die bisherigen Bereiche der zur Sicherung der persönlichen Lebensverhältnisse erforderlichen Daseinsvorsorge auch ein Verzicht auf das Social-Web als eine Art „soziale Grundversorgung" für Nutzer untragbar wird ohne kommunikative Ausgrenzung befürchten zu müssen ((Kamp and Rost, 2013, p. 82) a.A. Buchner, 2010, p. 41) wonach soziale Netzwerke noch kein unverzichtbarer Bestandteil des Soziallebens seien). Fehlende Alternativlösungen oder bestehende Gruppendynamiken und Netzwerkeffekte können dazu führen, dass ein Verzicht auf bestimmte Anwendungen mit einer eingeschränkten sozialen Anbindung einhergeht. Dann handelt es sich bei der Einwilligungserklärung lediglich noch um eine Fiktion (Kamp and Rost, 2013, p. 82; Roßnagel et al., 2001, p. 91; Seidel, 2014, p. 155).

Kopplungsverbote finden sich derzeit lediglich in § 28 Abs. 3b BDSG für die Datenverarbeitung im Rahmen des Adresshandels oder der Werbung. Hier wird die kommende Datenschutzgrundverordnung eine Verbesserung der Rechtslage für die Betroffenen erwarten lassen: Gerade Netzwerkeffekte (wie insbesondere bei sozialen Medien zu beobachten) oder fehlende Alternativangebote führen dazu, dass Nutzern häufig kaum eine vergleichbare Ausweichmöglichkeit verbleibt, wenn sie bei Nichtakzeptieren der Datenschutzeinstellungen auf das Angebot verzichten müssten. Die Position des Nutzers wird durch rechtliche Verbote gestärkt, die verbieten das Angebot von einer datenschutzrechtlichen Einwilligung in Datenerhebung abhängig zu machen, die für das Angebot nicht erforderlich ist. Art. 7 Abs. 4 DSGVO geht insoweit in die richtige Richtung, da eine solche Kopplung als Zwang gewertet werden kann, der zur Unwirksamkeit der Einwilligung führt. Echte Wahlfreiheit soll nach Erwägungsgrund 42 nur dann angenommen werden, wenn der Nutzer ohne Nachteile in der Lage ist, die Einwilligung zu verweigern.

Um nicht gänzlich auf die Anwendung verzichten zu müssen, wünschen sich nach einer europäischen Studie die Mehrheit der Befragten feingranularere Auswahlmöglichkeiten (Vodafone Institute for Society and Communication, 2016, p. 14). Obwohl die Befragten mehrheitlich Bereitschaft signalisieren, Daten für Verbesserungen bspw. in den Bereichen Gesundheit, Verkehr und Umwelt preiszugeben, lehnen sie eine pauschale Weitergabe der Daten an Dritte mehrheitlich ab. Mehr Transparenz und Kontrolle darüber wie welche Daten genutzt werden, könnte u.a. über knappere, einfach verständlichere Information sowie über technische Möglichkeiten Privatsphäreneinstellungen selbst vornehmen zu können, erreicht werden (Vodafone Institute for Society and Communication, 2016). Damit bestätigen die Nutzer eine Forderung der obersten Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich den Nutzern Möglichkeiten einzuräumen, aus der Nutzungssituation heraus individuell steuern zu können, welche Daten übertragen werden (Düsseldorfer Kreis, 2011, p. 1).

2.2.4.3.3 Bestimmtheit

Die Bestimmtheit der erklärten Einwilligung hängt entscheidend von der Granularität der übermittelten Informationen ab. Die Transparenz unterliegt insoweit dem Konflikt der Überforderung der Laien durch Aufzählung sämtlicher Datenflüsse, Verwendungszusammenhänge und Schutzmaßnahmen auf der einen Seite und der nur pauschalen, unkonkreten Umschreibung der geplanten Datenverwendung (Kamp and Rost, 2013, p. 83) wobei die Autoren davon ausgehen, dass vielfach die pauschale Umschreibung gewählt wird, um der verantwortlichen Stelle einen möglichst großzügigen Verwendungsspielraum zu eröffnen.). Damit der interessierte Nutzer die individuellen Risiken angemessen einzuschätzen vermag und gleichzeitig die Verständlichkeit unter verhältnismäßigem Wahrnehmungsaufwand gewahrt bleibt, wird daher ein gestaffeltes Vorgehen mit unterschiedlichen Informationsleveln

befürwortet (Kamp and Rost, 2013, p. 83). Eine pauschale „Generaleinwilligung“ wird i.d.R. als unwirksam eingestuft (Roßnagel, 2013). Die Artikel-29-Datenshutzgruppe geht in ihrer Stellungnahme zu Apps auf intelligenten Endgeräten davon aus, dass das bloße Bestätigen des „Installieren“-Buttons keinesfalls eine gültige Einwilligung darstellen kann, da dies keine Einwilligung in die konkret betroffenen Daten bzw. Datenkategorien darstellt und eine Einwilligung nicht auf bloß allgemein formulierter Autorisierung beruhen darf (Artikel-29-Datenschutzgruppe, 2013a, p. 19). Sie befürworten vielmehr Einwilligungen für den konkreten Fall, anstelle umfassender Datenschutzerklärungen/Nutzungsbedingungen.

2.2.4.4 Datensicherheit

Eine Testreihe des Fraunhofer-Instituts für sichere Informationstechnologie (SIT) stellte fest, dass von 10.000 getesteten Android-Apps 69% Daten unverschlüsselt über das Internet übertragen (Fraunhofer SIT, 2014). § 13 Abs. 4 Nr. 3 TMG normiert ausdrücklich, dass der Diensteanbieter durch technische und organisatorische Vorkehrungen sicherzustellen hat, dass der Nutzer Telemedien gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann. Unter der Einschränkung der technischen Möglichkeit und wirtschaftlichen Zumutbarkeit haben Diensteanbieter darüber hinaus nach § 13 Abs. 7 TMG im Rahmen ihrer jeweiligen Verantwortlichkeit für geschäftsmäßig angebotene Telemedien durch technische und organisatorische Vorkehrungen sicherzustellen, dass kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und diese gegen Verletzungen des Schutzes personenbezogener Daten und gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind, gesichert sind. Es wurde jedoch vom SIT bemängelt, dass bei rund 25 % der Apps die Entwickler wohl absichtlich auf Schutzfunktionen verzichteten und 12,5 % der Apps Daten an mehr als fünf Unternehmen verschicken, die mit der eigentlichen App-Funktion nichts zu tun haben (Fraunhofer SIT, 2014). Damit liegen in diesen Fällen Verstöße gegen § 13 TMG nahe. § 13 Abs. 7 S. 3 TMG nennt ausdrücklich den Einsatz eines als sicher anerkannten Verschlüsselungsverfahrens.

2.2.5 Datenschutzrechtliche Risiken des Webtrackings

Eine besondere Brisanz in der aktuellen Diskussion um Datenschutz und Apps nimmt das Webtracking ein. Hierbei handelt es sich um einen weltweiten Milliardenmarkt. Bei 72% von 400 untersuchten Smartphone-Apps wurden Tracking-Frameworks entdeckt (Schneider et al., 2014, p. 10). Unter Tracking-Technologie können Code-Elemente verstanden werden, die in Webseiten eingebettet sind und weitere Verbindungen im Hintergrund aufbauen. Folgende Technologien können zur Nutzerverfolgung eingesetzt werden: Cookies, Social Plugins, Geolokalisierung über IP-Adresse, Canvas Fingerprinting, E-Mail-Tracking, App-Tracking, Tastaturtracking (Dr. Datenschutz, 2015). Tracking-Technologien dienen bestimmten Funktionalitäten (z.B. Vereinfachung Webseitenaufruf, Warenkorb, Nutzerverhaltensanalyse, gezielte Werbung, Produktoptimierung, etc.) Ob Tracking für Nutzer von Vor- oder Nachteil ist, hängt maßgeblich vom Zweck des Einsatzes ab. Bspw. kann die Identifizierung durch Tastaturtracking neben Nutzername und Passwort als zusätzlicher Sicherheits-Faktor genutzt werden; aber auch zur Nachverfolgung des Nutzerverhaltens (Dr. Datenschutz, 2015; Kühl, 2015). Technische Gegenmaßnahmen durch Hardware wie e-Blocker (https://www.eblocker.com/de/); der „Tracking Protection“ im Browser / “Do-Not-Track”-Angabe (z.B. bei Firefox) gegenüber Webseiten bestehen grundsätzlich. Ein vollständiger technischer Selbstschutz wird derzeit allerdings als unmöglich eingestuft (Röttgen, 2016, p. 1). Dass es sich bei einer z.T. unbemerkten Profilbildung von Webseitenbetreibern auf Basis der Tracking-Technologien, sogar um einen schwerwiegenden Eingriff in den Schutzbereich handelt, ist unzweifelhaft (Düsseldorfer Kreis, 2009; Hören, 2011; Karg and Thomsen, 2012; Röttgen, 2016, p. 1; Schallaböck, 2014; Schleipfer, 2014; Schneider et al., 2014, p. 8). Tracking kann darüber hinaus Auswirkung auf Personen haben, die das Web nicht nutzen (Schneider et al., 2014, p. 7). Die Auswertung der

Profile kann die Informationsgewinnung über Interessen, politische Einstellungen, Bildungsgrad oder sexuelle Orientierung der Nutzer ermöglichen, und damit besonders sensible Daten (Röttgen, 2016, p. 1). Tracking wird teils für Nutzer unerwartet eingesetzt: z.B. Smart TV vor Aktivierung des Internetmodus (Schneider et al., 2014, p. 10); teils gegen den ausdrücklichen („Do-Not-Track"-Benachrichtigung)[14] oder konkludenten Willen: sog. „Zombie-Cookies", die sich bei Löschung widerherstellen (Röttgen, 2016, p. 2). Sobald über Tracking eine Profilbildung mit Wiedererkennung des Nutzers erfolgt, lassen sich die Daten konkreten Nutzern zuordnen und unterfallen als personenbezogene Daten dem Datenschutzrecht (Schneider et al., 2014, p. 8).[15] Soweit es sich um für die Ermöglichung oder Abrechnung der Inanspruchnahme von Telemedien erforderliche Daten handelt, wie bspw. Login-Session-Cookies, Warenkorb-Cookies oder Sicherheits-Cookies, ist die Datenverwendung mittels Tracking-Technologien legitim (Artikel-29-Datenschutzgruppe, 2012, p. 7 ff.; Schreibauer, 2014, sec. § 13 TMG Rn. 20). Alle weiteren Fälle bedürfen einer ausreichend informierten, aktiv und freiwillig erteilten Einwilligung zeitlich vor der Datenerhebung (Artikel-29-Datenschutzgruppe, 2013c, p. 3 ff).[16] Damit einher geht eine Hinweispflicht als weitere verfahrensrechtliche Sicherung der informationellen Selbstbestimmung (Düsseldorfer Kreis, 2009).

2.2.6 Zusammenfassung

Dieser generalisierende Überblick zeigt, dass in vielen Fällen davon ausgegangen werden kann, dass personenbezogene Daten datenschutzwidrig verwendet werden. Ob ein Datenschutzverstoß vorliegt, macht jedoch stets eine Einzelfallprüfung erforderlich. Oft fehlt es jedoch an einer praktischen Durchsetzung bestehender Rechte. Um private Nutzer bei der Wahrnehmung ihrer Rechte zu unterstützen, wurden bereits in der Vergangenheit Softwareanwendungen entwickelt, um eine bessere Kontrolle des Datenabflusses zu ermöglichen. Im Folgenden werden diese bereits vorhandenen Datenschutz-Apps auf ihre Bedienbarkeit, Funktionalität und Rechtskonformität hin untersucht.

3 Existierende Softwareanwendungen

Analog zu den oben beschriebenen Ansätzen in der Literatur lassen sich vorhandene Apps mit dem Anspruch, die Privatsphäre von Smartphonenutzern zu verbessern, in mehrere Kategorien einteilen:

Ratgeber: Diese Apps wollen den Nutzer in erster Linie informieren. Der am weitesten verbreitete Ansatz besteht darin, Apps nach ihrem Risiko für die Verletzung der Privatsphäre des zu bewerten (beispielsweise anhand der Berechtigungen, die sie verlangen). Auf diese Weise können gegebenenfalls Empfehlungen erteilt werden, welche Apps besser deinstalliert werden sollten.

Firewall: Weiterhin gibt es Apps, die nach dem Prinzip einer Firewall arbeiten. Diese sollen das Smartphone nicht nur vor Angriffen von außen, sondern explizit auch vor ungewollten Datenabflüssen schützen. Zu diesem Zweck kann beispielsweise der Internetzugang für eine bestimmte App oder die Verbindung zu bestimmten Servern blockiert werden. Ein anderer Ansatz wäre das Herausfiltern von bedenklichen Inhalten aus dem Datenverkehr, soweit dieser unverschlüsselt ist. Das Erfassen von Daten bspw. mittels GPS-Sensor wird nicht verhindert, jedoch werden die Kommunikationswege kontrolliert.

Manager: Zuletzt gibt es Apps, mit denen sich gezielt der Zugriff auf bestimmte Daten oder Funktionen für andere Apps blockieren oder einschränken lassen. Nach diesem Prinzip lässt sich sowohl der Zugriff

[14] Vgl. Datenschutzeinstellungen von Firefox; „Do-Not-Track-Flag" wird im Rahmen des Browser-Fingerprinting aber auch zur Verbesserung des Trackings genutzt: Fraunhofer SIT, Web-Tracking-Report 2014, S. 14.

[15] Die erwartete EuGH-Entscheidung zum Personenbezug von IP-Adressen könnte Anwendbarkeit noch ausweiten. BGH, EuGH-Vorlage vom 28. Oktober 2014 – VI ZR 135/13.

[16] Zum Einwilligungserfordernis bei Social-Plugins: LG Düsseldorf, Urteil vom 09. März 2016 – 12 O 151/15.

auf Daten, als auch der Abfluss von Daten verhindern, da beispielsweise auch für einzelne Apps der Internetzugang blockiert werden kann.

Die von PRIVACY-AVARE angestrebten Funktionalitäten sind: (1) Erfassen des Datenschutzprofils, (2) Verteilung des Datenschutzprofils, (3) Prüfung von Verletzungen des Datenschutzprofils und (4) Reduktion der Verletzung. **Ratgeber** Apps lassen sich grob der Funktion (3) zuordnen, und **Firewall** und **Manager** Apps den Funktionen (1), (3) und (4). Keine der identifizierten Apps erlaubt eine Verteilung der Präferenzprofils über mehrere Geräte hinweg (Funktionalität 2). Die konkrete Implementierung und gebotenen Möglichkeiten von Präferenzeinstellungen unterscheiden sich von App zu App, wobei **Manager** Apps der angestrebten Funktionalität von PRIVACY-AVARE am ehesten entsprechen. Um den Stand der Technik zu beurteilen, wurden daher **Manager**-Apps aus dem Google Play Store und aus externen Quellen identifiziert. Es wurden 18 Apps gefunden und untersucht. Zunächst kann festgestellt werden, dass sich diese Apps hinsichtlich ihrer Arbeitsweise, Benutzbarkeit und Funktionalität unterscheiden. Diese drei Aspekte werden daher im Folgenden vorgestellt. Tabelle 1 listet anschließend eine Übersicht zu allen betrachteten Apps und am Ende werden exemplarische Apps detailliert beschrieben.

3.1 Arbeitsweise der untersuchten Datenschutz-Apps

Das Einschränken einer App kann grundsätzlich durch zwei Herangehensweisen erreicht werden: entweder die Ausführungsumgebung wird eingeschränkt oder die auszuführenden Anwendungen werden modifiziert (Bishop, 2005). Konkret konnten die folgenden Ansätze identifiziert werden:

Manifest Datei (man): Soll eine Android-Anwendung auf Ressourcen des Smartphones zugreifen, beispielsweise auf Kontakte oder die Internetverbindung, so benötigt die Anwendung hierfür sogenannte Berechtigungen. Diese werden vom Benutzer erteilt. Die Informationen über die erfragten Berechtigungen sind in der sogenannten Manifest-Datei enthalten. Diese Datei ist Teil des Quellcodes, wird bei der Implementierung der Anwendung angelegt und enthält Meta-Informationen. Die untersuchten Apps manipulieren diese Manifest-Datei indem sie den Abschnitt über die zu erfragenden Berechtigungen ändern.[17] Dieses Vorgehen erfordert eine Neuinstallation der betroffenen Apps.

Hinzufügen einer Sicherheitsbibliothek (bib): Das Hinzufügen von Sicherheitsbibliotheken funktioniert folgendermaßen: Der Bytecode oder Quellcode der zu verändernden App wird hinsichtlich ihrer Methoden untersucht. Anschließend wird eigener Programmcode in den Bytecode oder Quellcode hinzugefügt. Der hinzugefügte Programmcode kann bestimmte Funktionsaufrufe protokollieren und überwachen. Hiermit wird folglich der Quellcode einer App verändert.

AppOps (ao): Das nachträgliche Entziehen von Berechtigungen oder selektive Erteilen von Berechtigungen wurde im Betriebssystem Android als Feature in der OS-Version 4.3 implementiert. Jedoch wurde diese Einstellungsmöglichkeit mit OS-Version 4.4.2 entfernt, bzw. versteckt. Einige untersuchte Anwendungen rufen die versteckte Einstellungsoption auf, um so dessen Funktionalität für den Benutzer wieder bereit zu stellen.

Custom-Rom (cr): Bei mobilen Betriebssystemen kann zwischen „Custom-ROM“ und „Stock-ROM“ unterschieden werden. Bei Letzteren handelt es sich um vom Hersteller vorinstallierte Betriebssysteme. Mit „Custom-ROM“ werden Betriebssysteme von Drittanbietern bezeichnet, die nicht ursprünglich vom Hersteller vorinstalliert wurden. Hierzu zählen auch die von Dritten modifizierten Android-

[17] Siehe den Abschnitt „uses-permission“ in der Beispiel-Manifest-Datei in Anhang 6.2.

Betriebssysteme wie beispielsweise CyanogenMod[18], Dirty Unicorns[19] oder PAC ROM[20]. Die Installation eines Custom-ROMs ist aufwendig und hängt vom Gerätehersteller und dem jeweiligen Custom-ROM ab.

XPosed (xp): Das XPosed Framework ermöglicht die Installation von verschiedenen Modulen, die das Betriebssystem (Stock-ROM) verändern können, ohne dass das Betriebssystem deinstalliert und durch ein sogenanntes Custom-ROM ersetzt werden muss. Es „ersetzt" das Android-Framework. Eines dieser Module ist das XPrivacy-Modul. Mit dem XPosed Framework kann man in jeden Prozess (d.h. in jede installierte App) eingreifen bzw. jede Methode zur Laufzeit verändern.

3.2 Benutzbarkeit der untersuchten Datenschutz-Apps

Die Beurteilung der identifizierten Apps erfolgt nach den übergeordneten Kriterien *Benutzbarkeit* und *Funktionalität*. Im Rahmen der Zielsetzung des AVARE Projektes meint Benutzbarkeit insbesondere *Benutzbarkeit für juristische und technische Laien*. Benutzbarkeit kann weiterhin nach den Aspekten Verständlichkeit (Wie leicht ist die Anwendung zu verstehen?), Erlernbarkeit (Wie viel Aufwand benötigt das Erlernen der Anwendung?), Bedienbarkeit (Wie viel Aufwand benötigt das Bedienen der Anwendung?), Attraktivität (Anziehungskraft der Software) und Konformität (Übereinstimmungsgrad der Software zu Normen und Vereinbarungen (ISO/IEC, 1991) unterschieden werden. Es war nicht Ziel dieser Untersuchung, eine komplette Bewertung und Analyse der Benutzbarkeit der Apps durchzuführen. In der Untersuchung wurde festgestellt, dass die Apps – je nach Implementierung und Arbeitsweise – den Nutzer bei der Installation und Bedienung vor gewisse Hürden stellen. Diese Aspekte fallen unter das oben beschriebene Konzept der Bedienbarkeit und werden im Folgenden dargestellt. Um eine einfache Bedienbarkeit für technische Laien zu erreichen, sollten die Hürden für die Installation der Manager-App, sowie für die Vornahme von Einstellungen, so gering wie möglich sein. Die folgenden potentiellen Hürden wurden identifiziert:

Root: Benötigt die App Root-Zugriff? (Das Freischalten des Root-Zugriffes, sogenanntes „Rooten", eines Android Smartphones kann bereits als technisch anspruchsvoll angesehen werden.)

Store: Ist die App im Google Play Store verfügbar? (Lässt sie sich also leicht und in der für den Benutzer gewohnten Weise installieren?)

Abhängigkeiten: Sind weitere technisch anspruchsvolle Abhängigkeiten zu erfüllen? Müssen beispielsweise zusätzliche Bibliotheken installiert werden, damit die App überhaupt funktioniert?

Neuinstallation: Ist für die Kontrolle einer App oder einer Einstellungsänderung eine Neuinstallation der betreffenden App erforderlich?

Updatefähigkeit: Bleiben einmal getroffene Einstellungen auch nach einem Update der kontrollierten App erhalten? (Bzw. ist ein Update einer kontrollierten App überhaupt möglich?)

Nutzeranforderungen: In welchem Maße muss ein Nutzer technisch versiert sein, um die App sinnvoll nutzen zu können?

[18] CyanogenMod ist ein modifiziertes Android-Betriebssystem, eine Community-Distribution von AOSP (Android Open Source Project).
[19] Dirty Unicorns verwendet seit Android 5.0 das AOSP als Basis für das modifizierte Betriebssystem.
[20] PAC-Rom vereint verschiedene Features verschiedener anderer alternativer, auf Android aufbauender, Betriebssysteme (z.B. CyanogenMod).

Für den Faktor **Nutzeranforderungen** wurden Noten vergeben, die in der folgenden Liste erläutert werden.

1: Die App erlaubt allgemeine oder abstrakte Einstellungen (z.B. Regelungen wie ``Stelle allen Apps statt meiner echten Kontaktdaten Schattendaten bereit.'')

2: Die App gibt Empfehlungen für Einstellungen (z.B. welchen Apps Berechtigungen entzogen werden sollen)

3: Die App erläutert mögliche Einstellungen.

4: Die App erlaubt lediglich, Einstellungen vorzunehmen.

5: Der Benutzer kann ohne technisches Wissen keine Einstellungen vornehmen.

``+'' oder ``-'' wurde vergeben, wenn die App das der Note entsprechende Benutzbarkeitsniveau (subjektiv) besonders gut oder vergleichsweise schlecht erfüllt.

3.3 Funktionalität der untersuchten Datenschutz-Apps

Alle untersuchten Datenschutz-Apps erlauben es, ein Datenschutzprofil zu erstellen. Hinsichtlich ihrer Funktionalität unterscheiden sich die betrachteten Datenschutz-Apps dahingehend, für welche persönlichen Daten sie den Zugriff verhindern oder beschränken. Zudem unterscheiden sich die Datenschutz-Apps noch darin, ob und wie sie den Abfluss von Daten verhindern.[21] Daraus ergeben sich die folgenden Kriterien:

Verhindert die App den *Zugriff* auf …

Kalender: z.B. Arzttermin

Kamera: z.B. unbemerkte Bildaufnahme

Kontakte: z.B. Telefonnummer von Bekannten

Ortsdaten: z.B. Bewegungsprofil

Mikrofon: z.B. unbemerkte Tonaufnahme

Sensoren: z.B. Gesundheitsdaten

SMS: z.B. persönliche Nachrichten

Speicher: z.B. persönliche Dokumente

Telefon: z.B. Anrufliste

Identität: z.B. eindeutige ID des Geräts

Apps: z.B. installierte Anwendungen

Verhindert die App den *Abfluss* von Daten über …

[21] Die Beurteilung erfolgt unabhängig davon, wie umfassend die entsprechende Kategorie persönlicher Daten tatsächlich geschützt wird. In einzelnen Fällen war bei der Untersuchung nicht ersichtlich, ob eine App tatsächlich alle möglichen Zugriffe auf Daten, die unter eine Kategorie fallen schützt. So werden unter der Kategorie „Telefon“ z.B. der „Telefonstatus“ und „Anrufliste“ zusammengefasst, manche Apps blockieren aber nur eines davon. Zudem ist es manchmal auch nicht eindeutig ersichtlich, was genau blockiert wird.

Bluetooth: Kommunikation mit anderen Bluetooth-Geräten

Internet: Zugriff auf das Internet per W-LAN oder Datennetz

NFC: Nahfeldkommunikation mit anderen Geräten

Systemapps: Können auch Systemapps kontrolliert werden?

Werbung: Wird speziell Werbung blockiert?

Tabelle 1 listet die Beurteilung aller Apps nach den *Zugriffs*- und *Abfluss*- sowie sonstigen Kriterien (**System**, **Werbung**). Neben dem reinen Verhindern eines Zugriffs (block), erlauben manche Apps die Einstellung, dass der Benutzer nach seiner Einwilligung gefragt wird (ask). In wenigen Fällen kann der Benutzer auch festlegen, dass Schattendaten übergeben werden sollen (fake)

				Usability						Funktionalität																
										Zugang											Abfluss			Sonstiges	
Name	Hersteller	Arbeitsweise	Quellcode	Root	Store	Abhäng.	Neuinst.	Updatefhg.	Nutzeranf.	Kalender	Kamera	Kontakte	Ortsdaten	Mikrofon	Sensoren	SMS	Speicher	Telefon	Identität	Apps	Bluetooth	Internet	NFC	Systemapps	Werbung
AppOps	*nativ*	ao	nein	ja	nein	nein	nein	?	4	b	b	b	b	b	b	b	b	b	b	b	b	b	b	ja	nein
APK Permission Remover	Steel-Works	man	ja	nein	ja	nein	ja	nein	3	b	b	b	b	b	b	b	b	b	b	b	b	b	b	nein	nein
Advanced Permission Manager	Steel-Works	man	ja	nein	ja	nein	ja	nein	3	b	b	b	b	b	b	b	b	b	b	b	b	b	b	nein	nein
SRT AppGuard	Backes SRT GmbH	bib	ja	nein	nein	nein	ja	ja	2	b	b	b	b	b	-	b	b	b	b	b	-	b	-	nein	nein
MoboClean	Mobo-Clean	bib	ja	nein	nein	nein	ja	ja	2+	-	-	a b	f b	-	-	a b	-	a b	a b	-	-	b	-	nein	nein
Privacy Protector	Houzuo Guo	?	nein	nein	ja	nein	nein	?	4	-	-	-	b	-	-	-	-	-	-	-	b	b	-	nein	nein
LBE Security Master	Lamian	xp	nein	ja	nein	nein	nein	?	2+	-	a, b	a, b	a, b	a, b	-	a, b	-	a, b	a, b	-	b	b	-	ja	ja
Parasol	Parasol .cool	?	?	ja	nein	nein	nein	?	2+	b	b	b	b	b	b	b	-	b	-	-	-	-	-	nein	nein
Gemini App Manager	SEASMIND	?	?	ja	ja	nein	nein	?	4	b	b	b	b	b	b	b	b	b	b	b	b	b	b	ja	nein
Permissions Denied	Stephen (Stericson)	?	?	ja	ja	nein	?	?	3	?	?	b	?	?	?	?	?	?	?	?	?	b	?	?	nein
App Guard	Ganesh Pokale	?	?	ja	ja	nein	?	?	3	?	?	?	?	?	?	?	?	?	?	?	b	b	?	?	nein
Pdroid	mateorod	cr	nein	ja	nein	ja	?	?	4	?	?	?	a, b, f	?	?	?	?	?	a, b, f	?	?	?	?	?	nein

XPrivacy	Marcel Bo-khorst	xp	nein	ja	ja	ja	nein	?	3-	a, b	a, b	a, b	a, b	a, b	a, b	a, b	a, b	a, b	a, b	a, b	?	a, b	a, b	nein	nein
Kapauer	Azalgo	xp	nein	ja		ja	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?
Permission Master	Droid Mate	xp	nein	ja	ja	ja	nein	?	3	b	b	b	b	b	b	b	b	b	b	b	b	b	b	nein	nein
3c Toolbox	3c	xp	nein	ja	ja	ja	nein	?	3-	b	b	b	b	b	b	b	b	b	b	b	b	b	b	ja	nein
MinMinGuard	FatMinMin	xp	nein	ja	nein	ja	nein	?	4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	?	ja
AdBlocker	Kubinkie	xp	nein	ja	nein	ja	nein	?	4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	?	ja

Tabelle 1: Übersicht Manager Apps

3.4 Detaillierte Beschreibung ausgewählter Datenschutz-Apps

Im Folgenden werden einige exemplarische Datenschutz-Apps mit unterschiedlichen Arbeitsweisen in Hinblick auf ihre Funktionsweise und den Funktionsumfang, sowie ihre Grenzen beschrieben.

3.4.1 SRT AppGuard

Die App ist nicht im Google Playstore verfügbar, sondern kann aus alternativen Quellen bezogen werden.[22] Für die Installation dieser App werden weder Root-Rechte noch ein Custom-ROM benötigt.

3.4.1.1 Funktionen

Die Funktionen der Applikation umfassen das Auflisten der installierten Anwendungen inklusive Details, eine Risikobewertung der Anwendungen und eine vom Anwender gestartete Überwachung. Zusätzlich werden die Aktivitäten der App geloggt und so nachvollziehbar gemacht.

3.4.1.2 Arbeitsweise

Die Risikobewertung erfolgt anhand der erteilten Berechtigungen. Je mehr „gefährliche“ Berechtigungen[23] eine Anwendung einfordert, desto größer wird der Risikowert. Die Werteskala liegt hier zwischen 1 und 10, wobei 1 unkritisch und 10 sehr kritisch bedeutet.

Die Überwachung einer Anwendung findet in 4 Schritten statt. Zunächst wird die Anwendung analysiert, anschließend wird der Benutzer zur Deinstallation aufgefordert. Danach wird der Anwendung *eine Sicherheitsbibliothek hinzugefügt*. Abschließend wird die Anwendung neu installiert. Nun können die Berechtigungen entfernt oder wieder hinzugefügt werden. Hierdurch kann sich die Risikobewertung verändern. Mit der Applikation können außerdem API-Aufrufe protokolliert werden. Ob der Funktionsaufruf durch AppGuard verhindert oder zugelassen wurde, wird ebenfalls gespeichert.

3.4.1.3 Grenzen

Nach den Angaben im Benutzerhandbuch (Backes SRT, 2014) ist der Funktionsumfang der Applikation dahingehend begrenzt, dass nicht alle von Android zuteilbaren Berechtigungen überwacht werden können (vgl. Tabelle 1). Außerdem können von SRT AppGuard überwachte Apps nicht über den Google Play Store aktualisiert werden. Dies ist auf die Änderungen, die SRT AppGuard am Quellcode der installierten und überwachten App durchführt, zurückzuführen. Um seine Anwendungen auf dem neuesten Stand halten zu können, muss man seinen Google-Account in den Einstellungen der App hinterlegen, damit sie die Update-Überprüfung durchführen kann. Durch das Deinstallieren der zu überwachenden Anwendung gehen deren Daten verloren. Auch beim Wiederherstellen gehen die Daten verloren, da die Anwendung deinstalliert wird.

Die App weist darauf hin, dass nur solche Anwendungen überwacht werden dürfen, deren Lizenzvereinbarung eine Modifikation zulässt. Ebenfalls nicht überwacht werden können Systemanwendungen und Funktionen, die mittels nativen Maschinencode aufgerufen werden. Anwendungen, die Google Maps verwenden und überwacht werden, erhalten keinen Zugriff mehr auf Google Maps.

3.4.2 Advanced Permission Manager

Die App „Advanced Permission Manager“ von SteelWorks ist aus dem Google Playstore installierbar.

---

[22] Beispielsweise hier: http://www.srt-appguard.com/ .

[23] Siehe die Beschreibung der von Android vorgenommenen Unterscheidung zwischen „normalen“ und „gefährlichen“ Berechtigungen auf Seite 4.

3.4.2.1 Funktionen

Der Anwender kann einzelne Berechtigungen suchen und erhält eine Liste von Anwendungen, denen diese Berechtigungen erteilt wurden. Auch eine Auflistung aller auf dem Endgerät installierten Anwendungen und vorhandener apk-Dateien ist möglich.

Das Entziehen von Berechtigungen ist ebenfalls mit dieser Applikation möglich. Der Anwender kann entweder nach den einzelnen Berechtigungen suchen (z.B. „SMS senden“) oder eine Anwendung auswählen und sich die Berechtigungen der App anzeigen lassen. Anschließend kann durch einen Klick auf die Berechtigung und ein anschließendes „Speichern & Neu installieren“ diese entzogen werden.

Eine Risikobewertung wird nicht durchgeführt, jedoch wird kurz erläutert welche Funktion die erteilte Berechtigung ausführen kann.

3.4.2.2 Arbeitsweise

Das Entziehen der Berechtigungen wird *durch Änderungen der jeweiligen Manifest-Datei*[24] einer Anwendung durchgeführt. Nachdem die Datei geändert wurde, muss die Anwendung neu installiert werden.

3.4.2.3 Grenzen

Die Applikation kann nicht allen installierten Anwendungen die Berechtigungen entziehen. Hierunter fallen beispielsweise die Google-Dienste und Systemanwendungen. Die Berechtigungen müssen jeder Anwendung einzeln entzogen werden. Weiterhin gehen durch das Deinstallieren und Neuinstallieren der Anwendung Daten und Einstellungen verloren.

Ein Hinweis auf mögliche Verstöße gegen Lizenzvereinbarung durch das Modifizieren der jeweiligen Anwendung erfolgt nicht. In der App selbst wird Werbung eingeblendet (im Testfall am unteren Rand des Bildschirms).

3.4.3 LBE Security Master

Die App „LBE Security Master“ ist lediglich im chinesischen Original aus dem Google Playstore installierbar. Eine deutsche Übersetzung kann aus einer anderen Quelle[25] heruntergeladen und auf dem Endgerät installiert werden. Für einige Funktionen werden Root-Rechte benötigt. Daher kann die Installation nur auf einem gerooteten Gerät erfolgen.

Die App selbst fordert 39 Berechtigungen wie beispielsweise „SMS senden“ und „Telefonnummer direkt anrufen“ und wurde vom SRT AppGuard mit einem Risikowert von 9,6 bewertet.

3.4.3.1 Funktionen

Die volle Funktionalität erhält man, wenn man den Aktivschutz aktiviert: Auf dem Home-Screen werden die Kategorien Tuning, App-Manager, Akku, Sicherheit und Privatsphäre und Internet angezeigt. Unter Tuning findet sich unter anderem ein Task Manager. Über diese Funktion kann der Speicher bereinigt und die CPU entlastet (Schließen von Tasks) werden. Über den App-Manager können apk-Dateien verwaltet, sowie Benutzer- und System-Apps deinstalliert werden.

[24] In der Manifest-Datei einer Android App muss der Entwickler unter anderem die Berechtigungen, die von der App benötigt werden, spezifizieren.
[25] Beispielsweise hier: http://beste-apps.chiS.de/android/app/lbe-security-master-android-app,cxo.67314552/ oder http://www.android-hilfe.de/thema/lbe-security-master-immer-aktuell.576790/.

Die App bietet weiterhin Viren-Scanner, einen Berechtigungsmanager und einen Werbeblocker. Der Berechtigungsmanager listet alle Apps auf und zeigt an, welche Berechtigungen die Anwendung benötigt. Es werden Empfehlungen ausgesprochen, ob eine Berechtigung erteilt oder verweigert werden soll.

Über das Menü kann der Aktivschutz aktiviert werden. Hierunter fallen Funktionen wie „Firewall“, „System App deinstallieren“, „Rechte Management“ und ein Protokoll von Berechtigungen. Hierfür werden Root-Rechte benötigt. Anwendungen können ohne Root-Berechtigung in einer Sandbox (hier als isolierte Umgebung beschrieben, aus welcher Anwendungen nicht heraus auf das System zugreifen können) ausgeführt werden. Außerdem kann man eine Anrufsperre einrichten. Hierunter fallen auch Funktionen mit denen Spam-SMS gemeldet werden können. Es gibt einen Firewall-Dienst, der SMS und Anrufe blockiert, eine Blacklist und eine Whitelist. Anrufe können individuell abgefangen werden (beispielsweise nach Anrufzeit).

Unter dem Menüpunkt „weitere Funktionen“ sind Unterpunkte wie Privatsphäre, Meldungen, Bezahldienst, Diebstahl und Kommunikation zu finden. Unter „Meldungen“ können Benachrichtigungen zu den vom Anwender installierten Applikationen ein oder ausgeschaltet werden. Die Funktion „Privatsphäre“ soll das Verschlüsseln von Dateien ermöglichen. Hierzu wird ein Entsperrmuster oder ein Passwort hinterlegt. Zusätzlich kann die Entsperrung per Gesichtserkennung oder NFC erfolgen. Es können Bilder, Videos und Dateien verschlüsselt werden. Anwendungen können gesperrt werden.

3.4.3.2 Arbeitsweise

Welche der in 3.1genannten Methoden verwendet wird, konnte durch die Verwendung der App nicht ermittelt werden. Auch die Beschreibung des Herstellers gibt wenig Hinweise auf die konkret verwendete Methode.

3.4.3.3 Grenzen

Während der Verwendung der Applikation wurde festgestellt, dass noch einige Übersetzungslücken bestehen. Im Test wurde bei Firefox die Funktion „Werbung“ ausgeschaltet. Wird Firefox gestartet, wird die Werbung jedoch weiter angezeigt.

3.4.4 XPrivacy

Die App „XPrivacy“[26] ist aus dem Google Playstore installierbar und Open Source unter einer GNU General Public Lizenz erhältlich. Für die Installation wird das XPosed Framework benötigt.

3.4.4.1 Funktionen

Die Applikation bietet folgende Funktionalitäten: Die vorhandenen Anwendungen werden aufgelistet. Für die Anwendungen verwendete Daten werden nach Kategorien sortiert. Diese können entsprechend beschränkt werden. Zu den Datenkategorien gehören beispielsweise: Accounts, E-Mail, Browser, Kalender und Location sowie Nachrichten und Netzwerk. Die Datenkategorien haben einzelne Funktionen. Diese können beschränkt oder nicht beschränkt werden. Die Funktionen sind farblich gekennzeichnet, wenn das Beschränken der Funktion zum Absturz der Anwendung führen kann. Einzelne Berechtigungen werden hier nicht entzogen.

[26] Eine ausführliche Dokumentation findet sich hier: https://github.com/M66B/XPrivacy#xprivacy .

Die App überwacht die Nutzung der Daten. Wird eine Datenkategorie von einer Anwendung verwendet oder versucht eine Anwendung eine Datenkategorie zu verwenden, so wird dies angezeigt. Außerdem gibt es für einzelne Datenkategorien die Möglichkeit, einer App falsche Daten anzubieten, beispielsweise wenn der App die Berechtigung zum Zugriff auf Kontaktdaten verweigert wird.

Auch die Berechtigungen von anderen Apps können mit XPrivacy gemanagt werden. Hierfür verwendet XPrivacy Mechanismen, insbesondere das Eingreifen in Funktionen, die das XPosed Framework bereitstellt. Des weiteren verwendet XPrivacy Funktionen, die Android zur Verfügung stellt (Beispiel: Verwendung von Parcel und AIDL zur Änderung von Berechtigungen).

XPrivacy macht sich zum Device Manager.

3.4.4.2 Arbeitsweise

XPrivacy ist ein *Modul für das XPosed Framework*. Es nutzt die Funktionalität von XPosed, um Funktionen von Android, die zur Laufzeit von einer App aufgerufen werden, zu modifizieren.

3.4.4.3 Grenzen

Die Grenzen der Anwendung werden unter (XPrivacy, 2016) detailliert aufgeführt. Im Folgenden werden einige genannt. Die Applikation entzieht keine Berechtigungen. Bestimmte Daten, wie beispielsweise die MAC Adresse, die IMEI oder die Seriennummer können nicht beschränkt werden. Lesezeichen und Verlauf des Browsers können für den Browser selbst nicht beschränkt werden. Die Telefonnummer kann für die vorinstallierte „Anruf“-Anwendung nicht beschränkt werden. Internet und Speicher können nur für Anwendungen, Provider und Dienste beschränkt werden, die vom Android Package Manager gestartet werden. Kalender und Kontakte können nicht für einzelne andere Anwendungen beschränkt werden, sondern entweder für alle oder für keine.

3.5 Rechtliche Implikationen

Derzeit sind bereits wie im ersten Teil des Berichts vorgestellt, diverse Selbstdatenschutz-Lösungen auch für Durchschnittsnutzer einsetzbar. Im Folgenden soll ein Überblick über mögliche rechtliche Implikationen dieser Anwendungen gegeben werden. Die rechtliche Bewertung kann im Einzelfall anhand der konkret gewählten technischen Ausgestaltung variieren, welche für den Normalnutzer in der Regel nicht einsehbar ist. Teils wird der Nutzer darauf hingewiesen, dass die Verantwortung der Rechtskonformität seiner Prüfung obliegt. So gibt SRT App Guard dem Nutzer einen Hinweis, dass Anwendungen nicht überwacht werden dürfen, die laut Lizenzvereinbarung vom Nutzer nicht Modifiziert werden dürfen. Hiermit zeigt sich ein nicht unerheblicher Nachteil für – weder technisch noch rechtlich versierte – Durchschnittsnutzer sowie die Praktikabilität für den Alltagseinsatz. Es ist anzunehmen, dass der Erfolg von Datenschutzlösungen entscheidend auch davon abhängt, wie hoch die an die Nutzer gestellten Anforderungen bezüglich Verständnis und nutzerfreundlicher Einsatzmöglichkeit ausfallen (Forum Privatheit, 2014, p. 15).

3.5.1 Urheberrecht

Entscheidend für die rechtliche Bewertung bestehender Selbstdatenschutz-Apps ist die konkrete technische Funktionsweise. Wird die Datenerhebung durch Dritt-Apps dadurch kontrolliert, dass proprietär geschützter Code verändert wird, stellt sich stets die Problematik, ob eine Urheberrechtsverletzung vorliegt (Bodden et al., 2013, p. 720; Brummund, 2014). Dies betrifft vornehmlich Modifikationen an den zu kontrollierenden Apps oder dem installierten Betriebssystem. Computerprogramme genießen grundsätzlich gemäß § 69a UrhG Urheberrechtsschutz, wenn sie individuelle Werke in dem Sinne darstellen, dass sie das Ergebnis der eigenen geistigen Schöpfung ihres Urhebers sind. Bei den meisten

Apps dürfte es sich unzweifelhaft um Computerprogramme i. S. d. § 69a UrhG handeln. Ob eine ausreichende geistige Schöpfungshöhe vorliegt, unterliegt der Einzelfallprüfung. Die Schwelle wird jedoch als relativ gering angesehen, sodass Urheberschutz die Regel und fehlende Schöpfungshöhe eher die Ausnahme darstellen soll (Brummund, 2014, p. 544; BT-Drs. 12 / 4022, S. 9). Da eine automatisierte Einzelfallprüfung durch die Selbstdatenschutzanwendung ausfällt und vom rechtlich nicht versierten Durchschnittsnutzer eine solche Prüfung ebenfalls nicht zu erwarten ist, sollte zur Herstellung von Rechtskonformität in sämtlichen Fällen vorsorglich für sämtliche Apps vom Vorliegen einer ausreichenden Schöpfungshöhe ausgegangen werden. Gemäß § 69c Nr. 2 UrhG steht zunächst nur dem Urheber das Recht die Bearbeitung, das Arrangement und andere Umarbeitungen eines Computerprogramms vorzunehmen. Liegen keine legitimierenden Lizenzen vor, ist Dritten die Veränderung des Computerprogramms grundsätzlich untersagt. Dem Urheber steht insoweit u.U. ein Unterlassungs- und/oder Schadensersatzanspruch nach § 97 Abs. 1 UrhG sowie ein Vernichtungsanspruch der zur Herstellung der widerrechtlichen Vervielfältigungsstücke verwendeten Vorrichtungen nach § 98 Abs. 1 S. 2 UrhG zu.

3.5.1.1 Veränderung der Manifestdatei

Bei Selbstdatenschutz-Lösungen wie bspw. dem Advanced Permission Manager wurde festgestellt, dass die Modifikation des Berechtigungsmanagements über die Löschung von Berechtigungseinträgen in der Manifestdatei erfolgt. Ein Urheberrechtseingriff könnte entweder vorliegen, wenn die Manifestdatei selbst urheberrechtlich geschützt ist oder ein Eingriff in die Gesamtanwendung anzunehmen ist. Grob enthalten Manifestdateien stets folgende Inhalte:

- Name der Anwendung
- Activities der App
- Zugelassene Nachrichtenübertragungen zwischen Apps
- Auflistung der Berechtigungen für Datenzugriffe durch die App

Die Manifestdatei könnte selbst ein gemäß § 69a Abs. 3 S. 1 UrhG für den Schutz erforderliches individuelles Werk in dem Sinne darstellen, dass sie das Ergebnis der eigenen geistigen Schöpfung ihres Urhebers ist. Computerprogramme sind gemäß § 1 (i) der Mustervorschriften der World Intellectual Property Organization (WIPO) als „eine Folge von Befehlen, die nach Aufnahme in einen maschinenlesbaren Träger fähig sind zu bewirken, dass eine Maschine mit informationsverarbeitenden Fähigkeiten eine bestimmte Funktion oder Aufgabe oder ein bestimmtes Ergebnis anzeigt, ausführt oder erzielt“ definiert. Da der Begriff weit zu verstehen ist, können auch Hilfsprogramme, Makros und Programmteile, wie Unterprogramme und Routinen, dem Begriff unterfallen (Dreier and Schulze, 2015, sec. § 69a Rn. 12; Kaboth and Spies, 2016, sec. § 69a Rn. 3; Wiebe, 2015, sec. § 69a UrhG Rn. 4) Dies gilt grundsätzlich ebenso für Schnittstellen, die als Bestandteil eines Computerprogramms die Verbindung und Interaktion mit anderen Programmen oder der Hardware ermöglichen (Kaboth and Spies, 2016, sec. § 69a Rn. 11). Ein eigenständiger Schutz eines solchen Programmteils besteht, sofern das Ergebnis einer eigenen geistigen Schöpfung des Urhebers vorliegt (Spindler et al., 2015, para. § 69a UrhG Rn. 5) Es bedarf einer menschlichen schöpferischen, d.h. gestalterischen Tätigkeit, die einen geistigen Gehalt aufweist, zu einer Formgestaltung geführt hat und eine hinreichende Individualität erkennen lässt (Dreier and Schulze, 2015, sec. § 69a Rn. 26). Insbesondere da Einträge in die Manifestdatei automatisch eingetragen werden können, bestehen durchaus Zweifel an einer eigenen menschlich-schöpferischen Tätigkeit. Bei mittels eines Computerprogramms generierten Computerprogrammen wird auf die Tätigkeit des das Ursprungsprogramm entwickelten Menschen zurückgegriffen (Dreier and Schulze, 2015, sec. § 69a Rn. 26). Eine kreative Gestaltung durch einen Menschen wäre höchstens über

die Auswahl der Einträge sowie den Programmablauf gegeben, welche sich jedoch eher an der Funktionalität orientieren dürften. Routinemäßig und von einer Vielzahl von Programmierern allgemein genutzte Programmbestandteile sind hingegen nicht geschützt (Dreier and Schulze, 2015, sec. § 69a Rn. 27). Denn nicht geschützt ist das, was sich aus der Natur der Aufgabe und aus rein funktionalen Erwägungen ergibt (vgl. OLG Düsseldorf, Urteil vom 27. März 1997 – 20 U 51/96; OLG Frankfurt, Urteil vom 09. September 1997 – 11 U 6/97; OLG München, Urteil vom 27. Mai 1999 – 6 U 5497/98; KG Berlin, Urteil vom 06. September 2010 – 24 U 71/10). Um einen umfassenden Werkschutz zu erreichen, wird die Grenze zwar recht weit gezogen, dies darf jedoch nicht dazu führen, dass gemeinfreie Bestandteile der freien Nutzbarkeit entzogen werden (OLG Hamburg, Urteil vom 12.03.1998 – 3 U 226/97).

Urheberrechtsschutz könnte jedoch bestehen, wenn die Manifestdatei als Bestandteil der Gesamtanwendung angesehen werden muss und sich dementsprechend die Bestimmung der Schöpfungshöhe der Anwendung als Ganzes folgt. Entscheidend ist der Begriff des „Computerprogramms“. DIN 44300 beschreibt ein Programm als „eine zur Lösung einer Aufgabe vollständige Anweisung zusammen mit allen erforderlichen Vereinbarungen“. Zur Vermeidung von Monopolisierung und Zugangsbeschränkungen zu allgemein bekanntem Wissen des Programmgestaltens, soll sich der urheberrechtliche Schutz aber nur auf solche inhaltlichen Elemente erstrecken, welche die Schutzvoraussetzung des § 69a Abs. 3 UrhG erfüllen (Dreier and Schulze, 2015, sec. § 69a Rn. 23). Es könnte aber ein Eingriff in das Gesamtwerk zu bejahen sein, auch wenn die Umarbeitung einen Bestandteil betrifft, der für sich alleine genommen keine schützenswerte Schöpfungsleistung darstellen sollte. Denn anders als die Vervielfältigung dieses (abtrennbaren) Programmbestandteils (die dann zulässig wäre), könnte eine Bearbeitung auch Auswirkungen auf das Gesamtwerkt haben. Brummund und Bodden et. al. gehen bei der von Datenschutz-Apps vorgenommenen Modifikation von einer zustimmungsbedürftigen Umarbeitung, i.S.d. § 69c Nr. 2 UhrG aus (Bodden et al., 2013, p. 722; Brummund, 2014, p. 544). Der Begriff der Umarbeitung ist weit zu verstehen (OLG Hamburg, Urteil vom 13.04.2012 – 5 U 11/11; Kaboth and Spies, 2016, sec. § 69c Rn. 10) Eine sonstige Programmänderung wie Erweiterung, Einschränkung und Ergänzung des Funktionsumfangs kann eine solche Umarbeitung darstellen (Dreier and Schulze, 2015, p. § 69c Rn. 15). Eine Änderung des Funktionsumfangs wie die Entfernung von Programmteilen unterfalle dementsprechend dem Bearbeitungsrecht (Bodden et al., 2013, p. 722). Eine Umarbeitung soll selbst dann vorliegen, wenn die Software die in einem externen Arbeitsspeicher programmgemäß abgelegten Daten verändert (OLG Hamburg Urteil vom 13.04.2012 – 5 U 11/11, GRUR-RR 2013, 13, 15 – Replay PSP). So entschied das OLG Hamburg, dass die Anpassung an individuelle Benutzerwünsche oder Erweiterungen des Funktionsumfangs eine lizenzpflichtige Umarbeitung darstellen, da dem Urheber das Recht zur Fortentwicklung und Anpassung seiner Software an unterschiedliche Nachfragerwünsche obliegt, selbst wenn die Umarbeitung über den Arbeitsspeicher dergestalt erfolgt, dass durch externe Befehle in den Programmablauf eingegriffen wird und kein Eingriff in die Programmsubstanz selbst gegeben ist (OLG Hamburg, Urteil vom 13.04.2012 – 5 U 11/11). Abzugrenzen ist diese Entscheidung von einer Entscheidung aus dem Jahr 1998/99: hier entschieden OLG Hamburg und OLG Düsseldorf, dass das Einspielen „falscher“ Daten keine Urheberrechtsverletzung darstellt, da die Daten keine Folge von Befehlen enthielten, die zur Kontrolle bzw. Steuerung des urheberrechtlich geschützten Computerprogramms benötigt werden (OLG Hamburg, Urteil vom 12.03.1998 – 3 U 226/97; OLG Düsseldorf, Urteil vom 12.7.1999 – 20 U 40/99) . Daraus lässt sich schließen, dass zu differenzieren ist, ob auf der einen Seite der Anwendung Befehle hinzugefügt oder entfernt werden und auf der anderen Seite nicht vorgesehene Daten eingespielt werden. Die Veränderung des Ablaufs der geschützten Software über die Manipulation der Daten im Arbeitsspeicher kam im Fall aus dem Jahr 2012 einer dauerhaften oder vorübergehenden Veränderung der verkörperten Software gleich, da das Spiel in seiner

Gesamtkonzeption verändert wurde (auch wenn die Spielidee keinen Urheberrechtsschutz genießt). Hier wäre ein Leerlaufen des Urheberrechts zu befürchten gewesen, da die der Klage zugrundeliegende Software „im Ergebnis einen Teil der Steuerung übernommen“ hat (OLG Hamburg, Urteil vom 13.04.2012 – 5 U 11/11). Die Gliederung des Programmablaufs, Anordnung der Programelemente sowie deren Zusammenwirken bei Computerprogrammen sind geschützt, (KG Berlin, Urteil vom 17. März 2010 – 24 U 117/08) und dieser Ablauf der programmierten Software wurde in einer vom Urheber nie vorgesehenen Weise verändert. Im Fall von 1998 wurde hingegen in die Ablaufroutine des Computerprogramms nicht eingegriffen (der Spieler konnte lediglich Level überspringen) (OLG Hamburg, Urteil vom 12.03.1998 – 3 U 226/97).

Werden Berechtigungen aus der Manifestdatei gelöscht, würde die App keine Datenzugriffsanfrage an das Betriebssystem stellen. Es liegt ein Eingriff in den Code der App und damit der Programmsubstanz vor. Die Frage wie der Programmablauf dadurch verändert wird, kommt es in diesem Fall dann nicht mehr an.

3.5.1.2 Hinzufügen einer Sicherheitsbibliothek

Durch Neuinstallation der zu überwachenden App wird durch SRT App Guard der App eine Sicherheitsbibliothek hinzugefügt. Hier gelten im Ergebnis ähnliche Erwägungen wie bei der Entfernung von Berechtigungen aus der Manifestdatei. Dem Programmcode der App wird zusätzlicher Code hinzugefügt, welcher Programmbefehle enthält und in den bestimmungsgemäßen Programmablauf der App eingreift. (vgl. auch LG Düsseldorf, Urteil vom 20. März 1996 – 12 O 849/93 zur Entfernung einzelner Programmfunktionen, die die Funktion des Gesamtprogramms wesentlich ändern (Dongle-Abfrage).

3.5.1.3 Veränderung des Betriebssystems

Eine weitere Möglichkeit besteht darin, über die Veränderung des Betriebssystems Datenabfragen der zu kontrollierenden App nicht umzusetzen. Ein permanentes Umschreiben des Betriebssystemcodes stellt zweifellos eine lizenzpflichtige Umarbeitung dar.

Bodden et.al. befürchten darüber hinaus, dass bei Bestätigung und Weiterdenkens der Entscheidung des OLG Hamburg vom 13.04.2012 (5 U 11/11) auch bei einer von der App nicht bedachten Verarbeitung ihrer Programmbefehle durch das Betriebssystem eine Umarbeitung anzunehmen wäre (Bodden et al., 2013, p. 723). Wenn bspw. der Programmbefehl „Sende folgende Daten an folgende Server“ vom Betriebssystem nicht umgesetzt, sondern ignoriert würde, würde der App-Code zwar intakt bleiben, der Ablauf der App könnte jedoch nicht so erfolgen, wie vom Urheber geplant. Wenn dies als Umarbeitung der App einzustufen wäre, stellen sich jedoch erhebliche Bedenken beim Zusammenwirken verschiedener Programme (Spindler, 2012, p. 419) Zieht man den Bearbeitungsbegriff zu weit, müssten sämtliche Interaktionen zwischen mehreren Anwendungen im Rahmen der Programmnutzung zunächst als Eingriffe gewertete werden und über § 69d UrhG legitimiert werden. Inwieweit dieser als Ausnahmeregelung lediglich notwendige Bearbeitungen zur Herstellung der bestimmungsgemäßen Nutzbarkeit oder auch zweckmäßig bzw. nützliche Bearbeitungen erfasst, ist umstritten (Dreier et al., 2015, sec. § 69d Rn. 11; Grützmacher, 2014, sec. § 69d Rn. 23). Daher wird ein tatsächlicher Eingriff in die Programmsubstanz gefordert (Grützmacher, 2014, sec. § 69c Rn. 20; Spindler, 2012) Entscheidend dürfte hier sein, ob durch Programmbefehle „im Ergebnis die Steuerung übernommen wird“ – welche vom Gewicht einem Eingriff in die Programmsubstanz gleichkommt - oder ob die Ablaufroutine grundsätzlich intakt bleibt.

Werden Datenzugriffsanfragen der App durch das Betriebssystem oder eine zwischengeschaltete Instanz ignoriert, läuft die App nach der vom Urheber vorgesehenen Ablaufroutine ab. Entweder die

Funktionsfähigkeit wird dadurch unterbunden, oder die App soll nach dieser Ablaufroutine trotz Nichtvorliegens der Daten weiterhin funktionieren. Die Funktionen einer Software werden nicht vom Urheberrecht geschützt (EuGH Urteil vom 02.05.2012 - Rs. C-406/10 - SAS Institute; Spindler, 2012, p. 417). In der Nichtansteuerung bestimmter Programme liegt lediglich ein Eingriff in deren nach außen in Erscheinung tretende Funktionen (KG Berlin, Urteil vom 06. September 2010 – 24 U 71/10). Eine Einschränkung des Funktionsumfangs folgt hier nicht durch einen Eingriff in die Programmsubstanz oder die App direkt steuernder Befehle, sondern durch das Fehlen der Daten. Diese könnten aber auch manuell vom Nutzer gar nicht generiert werden, oder durch äußere Einwirkungen nicht vorliegen. Werden Daten nicht manuell sondern automatisiert durch das (manipulierte) Betriebssystem blockiert, so ist eine abweichende Bewertung eher fernliegend. Ein „Leerlaufen des Urheberrechts“ ist in einem solchen Fall nicht zu befürchten. Die Gliederung des Programmablaufs, Anordnung der Programmelemente sowie deren Zusammenwirken dürften durch die blockierten Datenzugriffsanfragen nicht verändert werden.

3.5.1.4 Manipulation zur bestimmungsgemäßen Nutzung

Gemäß § 69d Abs. 1 UrhG bedürfen die in § 69c Nr. 1 und 2 genannten Handlungen nicht der Zustimmung des Rechtsinhabers, wenn sie für eine bestimmungsgemäße Benutzung des Computerprogramms einschließlich der Fehlerberichtigung durch jeden zur Verwendung eines Vervielfältigungsstücks des Programms Berechtigten notwendig sind und soweit keine besonderen vertraglichen Bestimmungen vorliegen. Brummund und Bodden et.al. ziehen diese Norm heran, um den zuvor festgestellten Eingriff in das Urheberrecht zu legitimieren (Bodden et al., 2013, p. 725; Brummund, 2014, p. 545). Dabei gehen sie davon aus, dass die kontrollierten Apps andernfalls in datenschutzrechtlich unzulässiger Weise Daten abfragen. Um eine bestimmungsgemäße und rechtmäßige Nutzung zu gewährleisten, seien die Modifikationen daher im Sinne des § 69d Abs. 1 UrhG notwendig (Brummund, 2014, p. 546). Grundlage der Annahme eines Datenschutzverstoßes ist hierbei die unzureichende Information, womit die Zustimmung zu Datenzugriffen keine wirksame Einwilligung im datenschutzrechtlichen Sinn darstellt. Diese Annahme unterliegt jedoch zwei Unsicherheiten: zum einen müssten tatsächlich sämtliche Apps vor der Installation lediglich unzureichende Information (auch in der Zukunft) bereitstellen und zum anderen dürften für die Datenerhebung keine gesetzlichen Erlaubnistatbestände einschlägig sein (sodass es einer wirksamen Einwilligung nicht bedarf). Bodden et.al. erörtern in diesem Zusammenhang die Wahrnehmbarkeit von Datenschutzerklärungen, welche insbesondere auf kleinen Bildschirmen beim Installationsvorgang kaum oder erst durch Scrollen sichtbar werden (Bodden et al., 2013, p. 723). Ob eine pauschalierte Annahme unzureichender Information einen Urheberrechtsverstoß legitimieren kann, ist jedoch durchaus zweifelhaft. Zudem sind Fallgestaltungen außerhalb der Anwendbarkeit des deutschen Datenschutzrechts denkbar, die nach dem jeweils anwendbaren Recht als datenschutzkonform zu betrachten wären.

Insbesondere in Fällen, in denen die Löschung der Zugriffsberechtigungen zur Unterbindung der Funktionsfähigkeit der App führt (z.B. ohne Zugriff auf das Adressbuch funktioniert WhatsApp nicht, da eine manuelle Dateneingabe nicht vorgesehen ist) stellen sich erhebliche Zweifel, Eingriffe in urheberrechtlich geschützten Code über § 69d UrhG zu legitimieren. Die bestimmungsgemäße Nutzbarkeit würde dann gerade nicht hergestellt.

3.5.1.5 Vorliegen legitimierender Lizenzen

Anders kann die Situation im Falle von Open Source zu bewerten sein, wenn die jeweils einschlägige Lizenz Bearbeitungen durch die Nutzer erlaubt. Die Open-Source-Bewegung hat sich zum Ziel gesetzt, den Quellcode des Programms offen zu legen und dessen Weiterverwendung, Veränderungen und

Weiterentwicklungen zu gestatten. Im Gegenzug werden die Nutzer verpflichtet, die Software nur unter den gleichen Bedingungen weiterzugeben (sog. Copyleft) (Dreier et al., 2015, sec. § 69a Rn. 5-11). Somit könnten Selbstdatenschutz-Anwendungen Apps oder das Betriebssystem anpassen, welche unter einer freie Bearbeitungen erlaubenden Open-Source-Lizenz vertrieben werden. Jedoch stellt es Nutzer vor nicht unbeachtliche Hürden, wenn sie bei jedem Einsatz der Selbstdatenschutz-App prüfen müssen, unter welchen Lizenzen diese angeboten werden.

3.5.2 Vertragsrecht

Abseits von Urheberrechtsverstößen könnte darüber hinaus in Veränderungen an zu kontrollierenden Apps oder dem Betriebssystem eine Verletzung der jeweiligen Lizenzvereinbarung liegen, wenn diese dem Nutzer rechtswirksam solche Veränderungen untersagt. Es wäre daher im Einzelfall zu prüfen, ob ein Lizenzvertrag mit einer derartigen Klausel vorliegt und ob diese rechtswirksam Bestandteil der Nutzungsvereinbarung zwischen App-Anbieter / Betriebssystem-Anbieter und Nutzer geworden ist. Handelt es sich um AGB, sind insbesondere die §§ 305 ff. BGB zu berücksichtigen.

4 Zusammenfassung und Ausblick

4.1 Kommende Rechtslage

Die rechtliche Einordnung von Selbstdatenschutz-Lösungen ist auch abhängig vom Grundverständnis der Kommerzialisierung (personenbezogener) Daten. Ist ein Geschäftsmodell so konzipiert, dass ein Dienst nicht gegen Entgelt sondern gegen Daten als Währung angeboten werden soll, stellt sich zunächst die Frage nach der datenschutzrechtlichen Zulässigkeit eines solchen Modells. Grundsätzlich handelt es sich um eine gesellschaftspolitische Problematik, ob ein solches Geschäftsmodell wirtschaftlich und kulturell erwünscht ist. Geprüft werden kann, inwieweit das Geschäftsmodell in Konflikt mit der Rechtsordnung steht. Generell kann sich hier ein Spannungsfeld zwischen zivilrechtlicher Dispositionsfreiheit und grundrechtlich gebotenem Datenschutz ergeben. Der Kommissionsentwurf einer Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte (COM 2015 / 634 final) sieht vor, personenbezogene Daten als Gegenleistung in einem Vertragsverhältnis anzuerkennen, soweit sie aktiv durch den Verbraucher bereitgestellt wurden – nicht hingegen bei passiver Preisgabe. Ob dieses Kriterium ein geeignetes und angemessenes Abgrenzungskriterium darstellt ist aufgrund der aktuellen Gestaltung der Datenerhebung insbesondere mittels Mobile-Apps eher zweifelhaft, da der Großteil der Daten für den Nutzer eher unbewusst erhoben werden dürfte. Zudem stellt sich die Frage der erforderlichen Transparenz für einen schuldrechtlich bindenden Vertrag sowie das Verhältnis zur Widerruflichkeit der Einwilligung (vgl. (BMWi, 2016, p. 58) Da eine Detailprüfung dieser Aspekte im weiteren Projektverlauf erfolgen soll, soll an dieser Stelle ein Überblick über den aktuellen Stand der Wissenschaft gegeben werden.

4.1.1 Das „Eigentum“ an Daten

Grundsätzlich gilt, dass mangels Sachqualität kein Eigentum i.S.d. BGB an Daten bestehen kann (Dorner, 2014; Duisberg, 2012; Hornung and Goeble, 2015, p. 268; Peschel and Rockstroh, 2014, p. 572; Zieger and Smirra, 2013, p. 419). Das gleiche dürfte auch für den „Datenbesitz“ gelten, da dieser tatsächliche Sachherrschaft voraussetzt. Dennoch werden häufig Modelle wie das „Data Ownership“ diskutiert (EU-Kommission nennt im Fahrplan zur Vollendung des digitalen Binnenmarkts als für 2016 geplante Maßnahme „Initiativen in Bezug auf das Eigentum an Daten, den freien Datenfluss (z.B. zwischen Cloud-Anbietern) und eine europäische Cloud“ in COM (2015) 192 final). Ein Ausschließlichkeitsrecht wird gerade in Bezug auf nicht-personenbezogene Daten diskutiert, insbesondere solche die ma-

schinengeneriert wie im Bereich Industrie 4.0 sind, in der Hoffnung dadurch vermeintliche Regelungslücken im Rechtsrahmen zu schließen (vgl. BDI and Noerr LLP, 2015, p. 12).[27] Die Meinungen in Literatur und Politik rangieren von:

- Herleitung eines Eigentums an Daten aus der Anwendung von § 303a StGB im Zivilrecht (Hoeren, 2013)
- Dateneigentum aufgrund Eigentum am Datenträger (weitgehend abgelehnt vgl. Dorner, 2014; Zech, 2015)
- Früchte oder Nutzungen einer Sache nach §§ 99, 100 BGB (Grosskopf, 2011)
- Schaffung eines Ausschließlichkeitsrechts aufgrund der wirtschaftlichen Leistung der „Datenerstellung" bzw. „Datenaufbereitung" (Zech, 2015)
- Daten als „sonstiges Recht" i. S. d. § 823 Abs. 1 BGB (Redeker, 2011)
- Orientierung am Urheberrecht für die Schaffung eines Datenverwertungsrechts (Schwartmann and Hentsch, 2015)
- Ablehnung eines Dateneigentums (Dorner, 2014).

Einige Autoren sprechen sich für die Schaffung einer den aktuellen Gegebenheiten Rechnung tragenden rechtlichen Regelungen einer „Dateneigentumsordnung" sowohl für personenbezogene als auch nicht-personenbezogene Daten aus (Fetzer, 2015, p. 778; Seidel, 2014). Hintergrund ist auch der Gedanke, dass über ein Datenwirtschaftsrecht bzw. die Bemessung der Daten als geldwerte Gegenleistung die Partizipation der Betroffenen an den Gewinnen ermöglicht und damit der Schutz der Betroffenen verbessert würde (Molavi, 2014, p. 80). Der Richtlinienentwurf (COM 2015 / 634 final) bleibt hinter einer solchen Forderung noch weit zurück. Schwartmann und Hentsch schlagen hingegen eine Orientierung am Urheberrecht vor (Schwartmann and Hentsch, 2015). Ob dadurch die von den Autoren bemängelte schwierige Rechtsdurchsetzung behoben wird, bleibt jedoch zweifelhaft. Wie die Rechteinhaber im Hinblick auf illegale Downloads ihre Rechte effektiver durchsetzen können, ist ebenfalls ein aktuell diskutiertes Problem. Soweit der Gesetzgeber den Forderungen zur Schaffung einer neuen Rechtsordnung nachkommen sollte, müssen die grundrechtlich geschützten Positionen der Nutzer angemessen berücksichtigt werden. Die Kommerzialisierung der hier maßgeblichen personenbezogenen Daten dürfte an der Unübertragbarkeit des allgemeinen Persönlichkeitsrechts und dem darin innewohnenden Menschenwürdekern scheitern (ausführlich: Buchner, 2006; Specht, 2012; Unseld, 2010). Somit wäre eine dingliche Übertragung von „Rechten an personenbezogenen Daten" mit der grundrechtlichen Ausgestaltung des Rechts auf informationelle Selbstbestimmung nicht vereinbar. Seidel verlangt daher eine Verfassungsreform (Seidel, 2014, p. 158). Hornung und Goeble konstatieren jedoch, dass

[27] Der Rechtsrahmen zum Schutz nicht-personenbezogener ist stark fragmentiert, sodass kaum von einem vollständig „rechtsfreien Raum" gesprochen werden kann. Datenverarbeitenden Stellen steht grundsätzlich je nach Erfüllung der Tatbestandsvoraussetzungen der Schutz von Datenbankwerken sowie das Datenbankherstellerrecht sui generis, der Schutz von Geschäfts- und Betriebsgeheimnissen sowie der Strafrechtsschutz zur Verfügung. Darüber hinaus wird der Datenumgang derzeit häufig auf vertraglicher Basis mit Wirkung inter partes in Zusammenwirken mit technischen Schutzmechanismen geregelt ((Specht, 2016, p. 289). Eine Gegenläufige hochaktuelle Diskussion bildet die Frage eines diskriminierungsfreien Zugangsrechts zu Datenplattformen und damit die Verhinderung von Marktzutrittsschranken und datengetriebener Marktmachtkonzentration. Die Schaffung neuer Ausschließlichkeitsrechte lässt vielmehr befürchten, dass bestehende Datenzugriffsmöglichkeiten wettbewerbshemmend zementiert werden. Vgl. (BDI and Noerr LLP, 2015, p. 12) Über die Zuweisung eines Ausschließlichkeitsrechts an der „Erzeuger" von Daten (z.B. dem Hersteller oder Eigentümer eines Sensors) besteht vielmehr die Gefahr, dass Produkthersteller Marktmacht in Sekundärmärkte verlagern und Lock-in-Effekte Wettbewerb verhindern. (BMWi, 2016) Vorgesehene Innovationen der DSGVO wie die Datenportabilität dürften auch zu mehr Wettbewerb führen und zu einem Ausschließlichkeitsrecht an Daten im Widerspruch stehen.

Nutzer bereits heute „eine zu geringe Gegenleistung“ erhalten und sich dies aufgrund der Informationsasymmetrien und Verhandlungsungleichgewichten zwischen Privatpersonen und weltweit operierenden Oligopolen auch bei verstärkt eigentumsrechtlicher Ausgestaltung des Datenschutzrechts kaum ändern wird (Hornung and Goeble, 2015, pp. 270, 271). Im Ergebnis könnte die rechtliche Anerkennung der Datenkommerzialisierung statt der erhofften Gewinnbeteiligung der Betroffenen vielmehr eine rechtliche Schlechterstellung bewirken. Insbesondere die am Urheberrecht orientierten dinglich wirkenden Nutzungslizenzen (Jöns, 2015; Schwartmann and Hentsch, 2015) schützen zunächst den Datenverwerter, da dieser eine gesicherte Rechtsposition (auch gegenüber dem Betroffenen) erhielte.

4.1.2 Das Geschäftsmodell „Dienst gegen Daten“

Obwohl eine zivilrechtliche Vertragseinordnung der Installation und Nutzung einer App, insbesondere wenn diese kostenlos erfolgt, noch umstritten ist, gehen einige Autoren von einem synallagmatischen Austauschverhältnis zwischen Dienst und Daten aus. (Bräutigam, 2012) Zum Teil wird vertreten, dass die datenschutzrechtliche Einwilligung genutzt werden könne, um eigene Daten als Zahlungsmittel einzusetzen (Buchner, 2010, p. 40). Dies könnte zu einer Art Tauschvertrag führen: die „(datenschutzrechtliche) Einwilligung gegen („kostenlose“) Leistung“ (Buchner, 2010, p. 39). Dann wäre entweder die Übertragung der Daten oder zumindest die Erteilung der Einwilligung als Hauptleistung in einem gegenseitigen Vertrag geschuldet und ein Abweichen könnte Regressansprüche des App-Anbieters verursachen.

Zum einen stellt sich die Frage, ob der aus Art. 2 Abs. 1, 1 Abs. 1 GG resultierende, staatliche Schutzauftrag, das Recht auf informationelle Selbstbestimmung auch gegenüber privaten Datenverwendern zu schützen, nicht zu einer Einschränkung der Dispositionsbefugnis führen muss. Aus dem Recht auf informationelle Selbstbestimmung folgt die staatliche Schutzpflicht der informationellen Selbstschutz für die Nutzer digitaler Dienste tatsächlich zu ermöglichen (BVerfG, stattgebender Kammerbeschluss vom 17. Juli 2013 – 1 BvR 3167/08) Die Möglichkeit sich vertraglich zur Preisgabe personenbezogener Daten zu verpflichten, könnte mit der Verantwortung des Staates die Voraussetzungen selbstbestimmter Kommunikationsteilhabe zu gewährleisten, kollidieren, wenn dadurch informationeller Selbstschutz nicht mehr möglich ist. (vgl. BVerfG, stattgebender Kammerbeschluss vom 23. Oktober 2006 – 1 BvR 2027 / 02) Auch unter grundsätzlicher Anerkennung der Dispositionsfreiheit muss das Recht darauf hinwirken, dass insbesondere bei Vertragspartnern mit überlegenem Verhandlungsgewicht eine einseitige Bestimmungsmacht dieses Vertragspartners nicht die grundrechtlich geschützte Selbstbestimmung in eine Fremdbestimmung verkehrt (BVerfG, stattgebender Kammerbeschluss vom 23. Oktober 2006 – 1 BvR 2027 / 02).

Zudem stellt sich bei einer schuldrechtlichen Bindung stets die Frage nach der Widerruflichkeit der datenschutzrechtlichen Einwilligung. So sieht der Richtlinienentwurf (COM 2015 / 634 final) vor, dass auch personenbezogene Daten als Gegenleistung digitaler Inhalte vom Verbraucher erbracht werden können und der Verbraucher den Vertrag nach Art. 12 Abs. 5 des Richtlinienentwurfs nur beenden darf, wenn Vertragswidrigkeit bezüglich der dort genannten Punkte besteht. Dies steht im krassen Widerspruch zur Widerruflichkeit und Freiwilligkeit der Einwilligung. Bezüglich der datenschutzrechtlichen Einwilligung ist zu erwarten, dass die Datenschutzgrundverordnung die Selbstbestimmung des Betroffenen insoweit stärkt, als dass Zweifel an der Freiwilligkeit der Einwilligung bestehen, wenn die Diensterbringung abhängig von der Einwilligung in die Datenverwendung nicht erforderlicher Daten gemacht wird (Art. 7 Abs. 4 DSGVO). Erwägungsgründe 42, 43 sollen Transparenz und Freiwilligkeit stärken, indem u.a. gefordert wird, dass die betroffene Person „eine echte oder freie Wahl hat und

somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden“ sowie ein „klares Ungleichgewicht“ zwischen Betroffenem und Verantwortlichem berücksichtigt werden muss. Darüber hinaus soll die Einwilligung nicht als freiwillig erteilt gelten, „wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist, oder wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist.“ Dies sollte als ein strenges Kopplungsverbot interpretiert werden.

Obwohl vielfach von Daten als neuer Währung gesprochen wird (z.B. BMWi, 2016, p. 32; Jöns, 2016) dürfte nicht allen Nutzern bewusst sein, dass ihre personenbezogenen Daten als Gegenleistung dienen und um welche Daten es sich dabei handelt (Vodafone Institute for Society and Communication, 2016). Dagegen gaben in einer deutschen Studie 47-76% der Befragten an bei „kostenlosen“ Angeboten mit ihren Daten zu „bezahlen“, wobei 56-80% dieses Vorgehen ablehnen und 73% angeben selten oder nie ihre Zustimmung hierzu zu erteilen (DIVSI, 2014, pp. 11, 16) 55% der befragten Europäer zieht es vor für Dienstnutzung mit Geld zu bezahlen (Vodafone Institute for Society and Communication, 2016, p. 21) Laut der DIVSI-Studie waren es im Jahr 2014 hingegen nur 1/3 der befragten Deutschen, wobei 59% jedoch kein Vertrauen haben, durch die Zahlung Datenschutz „erkaufen“ zu können. Dementsprechend forderten 71-86% der Befragten, dass Geschäfte mit personenbezogenen Daten gesetzlich verboten werden sollen (DIVSI, 2014, p. 22).

4.1.3 Ausblick

Inwieweit der Einsatz von (personenbezogenen) Daten als Währung rechtlich anerkannt wird und welche (schuld-)rechtlichen Verpflichtungen daraus erwachsen können, oder ob eine Art „Dateneigentumsordnung“ geschaffen werden soll, wird voraussichtlich die Entwicklung auf europäischer Ebene zeigen. Hierbei werden die unveräußerlichen Grundrechtspositionen der Betroffenen zu berücksichtigen sein. Um die bestehenden Rechte – insbesondere gegen marktmächtige Unternehmen oder die Daten monetarisierende Systeme - effektiv durchsetzen zu können, wird es technischer Lösungen zum Selbstdatenschutz bedürfen. Eine rechtsgebietsübergreifende Etablierung eines Selbstbestimmungsrechts bzw. Selbsthilferechts sollte Rechtssicherheit für technische Selbstdatenschutzlösungen ermöglichen. So sollten Codeveränderungen zu kontrollierender Anwendungen nicht als Eingriff in das Urheberrecht gewertet werden. Wenn App-Anbieter Nutzern keine echten Auswahlmöglichkeiten bieten, ob diese ihre personenbezogenen Daten oder eine Geldleistung als Entgelt für einen Dienst erbringen wollen, sollten datenschutzrechtliche Einwilligungen nicht als freiwillig erteilt gelten und insofern ein Selbsthilferecht erwachsen, nur die Daten preiszugeben, die für die Diensterbringung tatsächlich erforderlich sind. Selbst bei Anerkennung einer schuldrechtlichen Bindung zur Datenpreisgabe, fehlt es derzeit i.d.R. an der erforderlichen Transparenz, sodass die beim App-Angebot verwendeten Vertragsklauseln jedenfalls an einer AGB-Kontrolle scheitern dürften. Mit der kommenden Datenschutzgrundverordnung sind bereits folgende die Datensouveränität der Betroffenen steigernde Innovationen zu erwarten:

- Steigerung der Transparenz durch Standardisierung und Visualisierung (Art. 12 Abs. 7 DSGVO)

  Durch die Forderung der Maschinenlesbarkeit können Datenschutz-Anwendungen Nutzer dabei unterstützen ein Datenmanagement nach den individuellen Präferenzen umzusetzen, ohne dass Nutzer dies für jede installierte Anwendung separat durchführen müssen. Die Bildsymbolik dient zur Vereinfachung und die Standardisierung erlaubt Vergleichbarkeit mit Alternativangeboten. Die Norm ist jedoch freiwillig.

- Kopplungsverbot bei Legitimation durch Einwilligung sowie Pflicht zu echten Auswahlmöglichkeiten (Art. 7 Abs. 4 DSGVO, Erwägungsgründe 42, 43)

  Um die Selbstbestimmtheit einer Entscheidung Daten preiszugeben sicherzustellen, sollten personenbezogene Daten nicht als Gegenleistung für eine andere Leistung verlangt werden, insbesondere, wenn diese auf andere Weise nicht oder nur unter Schwierigkeiten erlangt werden kann. Echte Wahlfreiheit besteht nur dann, wenn gleichwertige Alternativen angeboten werden.

- Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Privacy-by-design, Art. 25 DSGVO)

  Die DSGVO nennt hier als „geeignete technische und organisatorische Maßnahmen" als Beispiel die Pseudonymisierung sowie als zu gewährleistende Datenschutzgrundsätze ausdrücklich die Datenminimierung. Trotz der Diskussion um die Angemessenheit des Grundsatzes der Datensparsamkeit in Zeiten des Datenreichtums (IT Gipfel-Fokusgruppe, 2015, p. 5) hält die DSGVO an diesem bewährten Prinzip fest. Eine weitere Neuerung stellt die Sanktionierung der Nichteinhaltung dieser Norm dar.

Weitere Forderungen sind bspw. die Etablierung eines „Identity-Managements" um die Persönlichkeitssphären (Intimsphäre, Privatsphäre, Öffentlichkeitssphäre) auch in der digitalen Welt mithilfe eines Pseudonym-Managements effektiv umzusetzen (BMWi, 2016, p. 60). ZU erforschen gilt es jedoch noch, wie ein Verknüpfen der unterschiedlichen Datenspuren technisch ausgeschlossen werden kann. Bspw. ist es bereits technisch möglich anhand des Schreibstils Texte unter verschiedenen Pseudonymen einer Person zuzuordnen (Goldschmidt and Bunk, 2016).

4.2 Gesamtbewertung der existierenden Softwareanwendung

Im Folgenden werden die Vor-und Nachteile der verschiedenen identifizierten technischen Ansätze diskutiert, um daraus Rückschlüsse für die technische und rechtswissenschaftliche Konzeption von PRIVACY-AVARE zu ziehen:

Das Entziehen von Berechtigungen über die *Modifikation der Manifest Datei* bringt in Hinblick auf die Benutzbarkeit für den Nutzer einige Nachteile: Für jede Berechtigungsänderung muss die betreffende App neu installiert werden – einmal getroffene Einstellungen gehen dabei verloren. Weiterhin erlaubt dieser Ansatz zwar die Vornahme von weitreichenden Einschränkungen (man kann einer App theoretisch sämtliche Berechtigungen entziehen) – dies kann aber dazu führen, dass die App unvorhersehbar abstürzt oder gänzlich unbenutzbar wird. Es können auch nur Zugriffe oder Abflüsse unterbunden werden – ein Bereitstellen von Schattendaten oder eine Abfrage der Nutzerpräferenzen zur Laufzeit ist mit diesem Ansatz nicht möglich. Dieser Ansatz geht mit urheberrechtlichen Risiken einher, da die Modifikation der Manifest Datei einen Eingriff in die Programmsubstanz darstellt.

Der von einer App wie beispielsweise SRT AppGuard verfolgte Ansatz ist *das Hinzufügen einer Sicherheitsbibliothek*. Die App ist für den Benutzer komfortabler, da kontrollierte Apps jeweils nur einmal neu installiert werden müssen und Einstellungen auch über ein Update der betreffenden App erhalten bleiben. Um dies zu gewährleisten, ist allerdings ein erheblicher Mehraufwand in der Entwicklung erforderlich. Theoretisch lassen sich über diesen Ansatz die Zugriffe und Berechtigungen einer App beliebig kontrollieren. Auch dies ist mit erheblichem Entwicklungsaufwand verbunden, was sich auch darin zeigt, dass Apps, die einen entsprechenden Ansatz verfolgen, (noch) nicht alle relevanten Zugriffe

oder Abflüsse kontrollieren können (vgl. SRT AppGuard und MoboClean in Tabelle 1). Aus urheberrechtlicher Sicht stellt das Hinzufügen einer Sicherheitsbibliothek ebenfalls einen Eingriff in die Programmsubstanz dar.

Alle Apps, die Modifikationen am Betriebssystem vornehmen (*XPosed, custom rom*) stellen den Nutzer vor größere Hürden bei der Installation. Nach der Installation eröffnet sich zwar theoretisch jede Möglichkeit der Kontrolle (die App XPrivacy in Tabelle 1 hat den wohl größten Funktionsumfang der identifizierten Apps) – dafür ist allerdings das Rooten des Geräts und die Installation von zusätzlichen Abhängigkeiten notwendig. Zum einen muss die Lizenz auch hier die Umarbeitung durch den Nutzer erlauben. Zum anderen kommen diese Anforderungen für den Nutzer mit zusätzlichen Risiken, wie dem Verlust der Garantie oder irreperablen Schäden am Gerät.

Insgesamt wird deutlich, dass vorhandene Datenschutzapps, die vielfältigen Herausforderungen in Bezug auf Benutzbarkeit, Funktionalität und rechtliche Fragen noch nicht zufriedenstellend lösen.

5 Literaturverzeichnis

Analysis and impact study on the implementation of Directive EC 95/46 in Member States, 2003.

Artikel-29-Datenschutzgruppe, 2013a. Stellungnahme 02/2013 zu Apps auf intelligenten Endgeräten - WP 202.

Artikel-29-Datenschutzgruppe, 2013b. Opinion 03/2013 on Purpose Limitation - WP 203.

Artikel-29-Datenschutzgruppe, 2013c. Arbeitsunterlage 02/2013 mit Leitlinien für die Einholung der Einwilligung zur Verwendung von Cookies - WP 208.

Artikel-29-Datenschutzgruppe, 2012. Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht - WP 194.

Backes SRT, 2014. SRT AppGuard Benutzerhandbuch.

Barnitzke, B., 2010. Herausgabe von IP-Adressen: Eine datenschutzrechtliche Bewertung der Entscheidung des OLG Hamburg, Urteil vom 2.7.2008 - 5 U 73/07. Datenschutz Datensicherheit - DuD 34, 482–485. doi:10.1007/s11623-010-0135-y

Baumgartner, U., Ewald, K., 2016. Apps und Recht, 2. Auflage. ed. C.H. Beck, München.

BDI, Noerr LLP (Eds.), 2015. Industrie 4.0 – Rechtliche Herausforderungen der Digitalisierung.

Beisenherz, G., Tinnefeld, M.-T., 2011. Aspekte der Einwilligung: Zivil- und strafrechtliche Bezüge der Einwilligung im Datenschutzrecht. Datenschutz Datensicherheit - DuD 35, 110–115. doi:10.1007/s11623-011-0029-7

Bishop, M., 2005. Introduction to computer security. Addison-Wesley, Boston.

Bizer, J., 2007. Sieben Goldene Regeln des Datenschutzes. Datenschutz Datensicherheit - DuD 31, 350–356. doi:10.1007/s11623-007-0133-x

BMWi, 2016. Grünbuch Digitale Plattformen.

Bodden, E., Rasthofer, S., Richter, P., Roßnagel, A., 2013. Schutzmaßnahmen gegen datenschutz- unfreundliche Smartphone-Apps: Technische Möglichkeiten und rechtliche Zulässigkeit des Selbstdatenschutzes bei Apps. Datenschutz Datensicherheit - DuD 37, 720–725. doi:10.1007/s11623-013-0300-1

Bräutigam, P., 2012. Das Nutzungsverhältnis bei sozialen Netzwerken - Zivilrechtlicher Austausch von IT-Leistung gegen personenbezogene Daten. MMR 635–641.

Breyer, P., 2009. Verkehrssicherungspflichten von Internetdiensten im Lichte der Grundrechte. MMR 14–19.

Brummund, A., 2014. Smartphones und Apps: Datenschutzrechtliche Risiken und deren Begrenzung. GI Jahrestag. 539–550.

Buchner, B., 2010. Die Einwilligung im Datenschutzrecht: — vom Rechtfertigungsgrund zum Kommerzialisierungsinstrument. Datenschutz Datensicherheit - DuD 34, 39–43. doi:10.1007/s11623-010-0010-x

Buchner, B., 2006. Informationelle Selbstbestimmung im Privatrecht, Jus privatum. Mohr Siebeck, Tübingen.
Buggisch, W., 2004. Fälschung beweiserheblicher Daten durch Verwendung einer falschen E-Mail-Adresse? NJW 3519–3522.
Chun, B.-G., Jung, J., Enck, W., Gilbert, P., Cox, L.P., McDaniel, P., Sheth, A.N., 2010. TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones.
Dammann, U., 2014. Bundesdatenschutzgesetz, 8., neu bearbeitete Auflage. ed, NomosKommentar. Nomos, Baden-Baden.
DIVSI (Ed.), 2014. DIVSI Studie Daten – Ware und Währung.
Dorner, M., 2014. Big Data und „Dateneigentum“. Comput. Recht 30, 617–628. doi:10.9785/cr-2014-0909
Dr. Datenschutz, 2015. Neue Tracking-Methoden: Tastatur-Eingaben und Akku-Ladestand. Datenschutzbeauftragter Info.
Dreier, T., Schulze, G., 2015. Urheberrechtsgesetz: Urheberrechtswahrnehmungsgesetz, Kunsturhebergesetz: Kommentar, 5. Auflage. ed. C.H. Beck, München.
Dreier, T., Schulze, G., Specht, L., 2015. Urheberrechtsgesetz: Urheberrechtswahrnehmungsgesetz, Kunsturhebergesetz ; Kommentar, 5. Aufl. ed. C.H. Beck, München.
Duisberg, A., 2012. Wem gehören die Daten und wer hat außerdem Rechte daran?, in: Eberspächer, J., Wohlmuth, O. (Eds.), Big Data Wird Neues Wissen. Münchener Kreis e.V., p. 36 ff.
Düsseldorfer Kreis, 2011. Datenschutzgerechte Smartphone-Nutzung ermöglichen.
Düsseldorfer Kreis, 2009. Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten.
Eckhardt, J., 2015. Recht der elektronischen Medien: Kommentar, 3. Aufl. ed. Beck, München.
Felt, A.P., Chin, E., Hanna, S., Song, D., Wagner, D., 2011a. Android permissions demystified, in: Proceedings of the 18th ACM Conference on Computer and Communications Security. ACM, pp. 627–638.
Felt, A.P., Greenwood, K., Wagner, D., 2011b. The effectiveness of application permissions, in: Proceedings of the 2nd USENIX Conference on Web Application Development. pp. 7–7.
Fetzer, T., 2015. Plädoyer für ein neues Datenrecht. MMR 777–778.
Forum Privatheit, 2014. White Paper Selbstdatenschutz.
Fraunhofer SIT, 2014. Tausende Apps zu unsicher für Einsatz in Unternehmen - App-Entwickler verzichten absichtlich auf Sicherheitsfunktionen [WWW Document]. URL https://www.sit.fraunhofer.de/de/news/aktuelles/presse/details/news-article/app-entwickler-verzichten-absichtlich-auf-sicherheitsfunktionen/ (accessed 4.30.16).
FUTURE OF PRIVACY FORUM, 2012. FPF Mobile Apps Study.
Gabriel, U., Albrecht, S., 2010. Filesharing-Dienste, Grundrechte und (k)eine Lösung? ZUM 5, 392–397.
Gartner, 2015. Smartphones - Marktanteile der Betriebssysteme am Absatz bis 2015 | Statistik [WWW Document]. Statista. URL http://de.statista.com/statistik/daten/studie/12885/umfrage/marktanteil-bei-smartphones-nach-betriebssystem-weltweit-seit-2009/ (accessed 6.21.16).
Goldschmidt, P., Bunk, P., 2016. Big Data und die Dual-Use Problematik am Beispiel öffentlicher Daten. Datenschutz Datensicherheit - DuD 1.
Google, 2016. System Permissions | Android Developers [WWW Document]. URL https://developer.android.com/guide/topics/security/permissions.html (accessed 6.21.16).
Grosskopf, L., 2011. Rechte an privat erhobenen Geo- und Telemetriedaten. IP-Beratungspraxis 11, 259–261.
Grützmacher, M., 2014. Praxiskommentar zum Urheberrecht, 4., neu bearb. Aufl., Gesetzesstand 1. April 2014. ed. Beck, München.
Hoeren, T., 2013. Dateneigentum Versuch einer Anwendung von § 303a StGB im Zivilrecht. MMR 486–491.
Hören, T., 2011. Google Analytics - datenschutzrechtlich unbedenklich? ZD 3.

Hornung, G., Goeble, T., 2015. „Data Ownership“ im vernetzten Automobil. Comput. Recht 31, 265–273. doi:10.9785/cr-2015-0407
Hornyack, P., Han, S., Jung, J., Schechter, S., Wetherall, D., 2011. These aren’t the droids you’re looking for: retrofitting android to protect data from imperious applications, in: Proceedings of the 18th ACM Conference on Computer and Communications Security. ACM, pp. 639–652.
IRISS, 2015. European Policy Brief - Recommendations to the Council of the EU and the European Parliament on access rights, in the context of the European data protection reform.
ISO/IEC, 1991. ISO/IEC 9126.
IT Gipfel-Fokusgruppe, 2015. Leitplanken Digitaler Souveränität.
Jöns, J., 2016. Daten als Handelsware.
Jöns, J., 2015. Reformbedarf beim Datenschutzrecht [WWW Document]. DIVSI Dtsch. Inst. Für Vertrauen Sicherh. Im Internet. URL https://www.divsi.de/reformbedarf-beim-datenschutzrecht/
Kaboth, D., Spies, B., 2016. BeckOK Urheberrecht. C.H. Beck, München.
Kamp, M., Rost, M., 2013. Kritik an der Einwilligung: Ein Zwischenruf zu einer fiktiven Rechtsgrundlage in asymmetrischen Machtverhältnissen. Datenschutz Datensicherheit - DuD 37, 80–84. doi:10.1007/s11623-013-0022-4
Karg, M., Thomsen, S., 2012. Tracking und Analyse durch Facebook: Das Ende der Unschuld. Datenschutz Datensicherheit - DuD 36, 729–736. doi:10.1007/s11623-012-0240-1
Karger, M., 2010. Selbstdatenschutz Online: Die Deutschen sind die eifrigsten Schwindler.
Kremer, S., 2012. Datenschutz bei Entwicklung und Nutzung von Apps für Smart Devices. Comput. Recht 28. doi:10.9785/ovs-cr-2012-438
Kremer, S., Hoppe, A., Kamm, K., 2015. Apps und Kartellrecht. Comput. Recht 31. doi:10.9785/cr-2015-0106
Kühl, E., 2015. Deine Tastatureingaben verraten dich. Zeit Online.
Lin, J., Amini, S., Hong, J.I., Sadeh, N., Lindqvist, J., Zhang, J., 2012. Expectation and purpose: understanding users’ mental models of mobile app privacy through crowdsourcing, in: Proceedings of the 2012 ACM Conference on Ubiquitous Computing. ACM, pp. 501–510.
Liu, B., Liu, B., Jin, H., Govindan, R., 2015. Efficient Privilege De-Escalation for Ad Libraries in Mobile Apps. ACM Press, pp. 89–103. doi:10.1145/2742647.2742668
Molavi, R., 2014. Das Netz 2014/2015: Jahresrückblick Netzpolitik. iRights Media, Berlin.
Moos, F., 2010. Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG: und zu den Datenschutzvorschriften des TKG und TMG, 1. Aufl. ed, Schriftenreihe Kommunikation & Recht. Verl. Recht und Wirtschaft, Frankfurt, M.
Müller-Broich, J.D., 2012. Telemediengesetz, 1. ed, NOMOS Kommentar. Nomos.
Nauman, M., Khan, S., Zhang, X., 2010. Apex: extending android permission model and enforcement with user-defined runtime constraints, in: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. ACM, pp. 328–332.
Nordemann, J.B., 2010. Anmerkung zu OLG Düsseldorf, Urteil vom 27. April 2010 - I-20 U 166/09 - Rapidshare. ZUM 604–606.
Norton, 2011. Norton Cybercrime Report.
Peschel, C., Rockstroh, S., 2014. Big Data in der Industrie Chancen und Risiken neuer datenbasierter Dienste. MMR 571–576.
Plath, K.-U. (Ed.), 2013. BDSG: Kommentar zum BDSG sowie den Datenschutzbestimmungen von TMG und TKG. O. Schmidt, Köln.
Redeker, H., 2011. Information als eigenständiges Rechtsgut. Comput. Recht 27, 634–639. doi:10.9785/ovs-cr-2011-634
Richter, P., 2014. Ein anonymes Impressum? Profile in sozialen Netzwerken zwischen Anbieterkennzeichnung und Datenschutz. MMR 517.
Rockstroh, S., 2013. Impressumspflicht auf Facebook-Seiten Wann werden Telemedien „in der Regel gegen Entgelt” angeboten? MMR 627.
Roßnagel, A., 2013. Big Data - Small Privacy? ZD 11, 562–567.

Roßnagel, A., Pfitzmann, A., Garstka, H., 2001. Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Innern.
Röttgen, C., 2016. Gefällt mir, gefällt mir nicht - Tracking im Internet.
Schaar, P., 2001. Datenschutzrechtliche Einwilligung im Internet. Multimed. Recht 10, 644.
Schallaböck, J., 2014. Was ist und wie funktioniert Webtracking? IRights Info.
Schleipfer, S., 2014. Facebook-Like-Buttons: Technik, Risiken und Datenschutzfragen. Datenschutz Datensicherheit - DuD 38, 318–324. doi:10.1007/s11623-014-0118-5
Schnabel, C., Freund, B., 2010. „Ach wie gut, dass niemand weiß ...“ – Selbstdatenschutz bei der Nutzung von Telemedienangeboten. Comput. Recht 26. doi:10.9785/ovs-cr-2010-718
Schneider, M., Enzmann, M., Stopczynski, M., Waidner, M., 2014. Web-Tracking-Report 2014, SIT Technical Reports. Fraunhofer Verl, Stuttgart.
Schreibauer, M., 2014. BDSG: Kommentar zum Bundesdatenschutzgesetz: Nebengesetze, 4. Auflage. ed, Heymanns Kommentare. Carl Heymanns Verlag, Köln.
Schwartmann, R., Hentsch, C.-H., 2015. Eigentum an Daten - Das Urheberrecht als Pate für ein Datenverwertungsrecht. RDV 221–230.
Seidel, U., 2014. Das Grundrecht auf Datensouveränität. ZG 153–165.
Simitis, S., 2014. Bundesdatenschutzgesetz, 8., neu bearbeitete Auflage. ed, NomosKommentar. Nomos, Baden-Baden.
Smith, E., 2010. iPhone applications & privacy issues: An analysis of application transmission of iPhone unique device identifiers (UDIDs). URL Www Pskl Uswpwp-Contentuploads201009iPhone-Appl.-Priv.-Issues Pdf.
Solmecke, C., Taeger, J., Feldmann, T., Denker, C. (Eds.), 2013. Mobile Apps: Rechtsfragen und rechtliche Rahmenbedingungen, De Gruyter Praxishandbuch. De Gruyter, Berlin.
Specht, L., 2016. Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen. Comput. Recht 32, 288–296. doi:10.9785/cr-2016-0504
Specht, L., 2012. Konsequenzen der Ökonomisierung informationeller Selbstbestimmung: die zivilrechtliche Erfassung des Datenhandels, Karlsruher Schriften zum Wettbewerbs- und Immaterialgüterrecht. Heymanns, Köln.
Spindler, G., 2012. Grenzen des Softwareschutzes. Comput. Recht 28. doi:10.9785/ovs-cr-2012-417
Spindler, G., Nink, J., 2015. Recht der elektronischen Medien: Kommentar, 3. Aufl. ed. Beck, München.
Spindler, G., Schuster, F., Döpkens, H.-R. (Eds.), 2015. Recht der elektronischen Medien: Kommentar, 3. Aufl. ed. Beck, München.
Stevens, R., Gibler, C., Crussel, J., Erickson, J., Chen, H., 2011. Investigating User Privacy in Android Ad Libraries, in: Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems. ACM Press, Vancouver, BC, Canada.
Unseld, F., 2010. Die Kommerzialisierung personenbezogener Daten, Rechtswissenschaftliche Forschung und Entwicklung. Utz, München.
Vodafone Institute for Society and Communication, 2016. BIG DATA – a European survey on the opportunities and risks of data analytics.
Weichert, T., 2013. Big Data und Datenschutz. ZD 6, 251–259.
Wiebe, A., 2015. Recht der elektronischen Medien: Kommentar, 3. Aufl. ed. Beck, München.
Wolff, H.A., Brink, S., Albers, M., Wolff-Brink (Eds.), 2013. Datenschutzrecht in Bund und Ländern: Grundlagen. Bereichsspezifischer Datenschutz. BDSG ; Kommentar. Beck, München.
XPrivacy, 2016. XPrivacy - Limitations [WWW Document]. GitHub. URL https://github.com/M66B/XPrivacy (accessed 6.21.16).
Zech, H., 2015. Daten als Wirtschaftsgut – Überlegungen zu einem „Recht des Datenerzeugers“. Comput. Recht 31, 137–146. doi:10.9785/cr-2015-0303
Zieger, C., Smirra, N., 2013. Fallstricke bei Big Data-Anwendungen Rechtliche Gesichtspunkte bei der Analyse fremder Datenbestände. MMR 418–421.
Zscherpe, K., 2010. Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG: und zu den Datenschutzvorschriften des TKG und TMG, 1. Aufl. ed, Schriftenreihe Kommunikation & Recht. Verl. Recht und Wirtschaft, Frankfurt, M.

6 Anhang

6.1 Desktopbasierte Analysetools

Name der Implementierung	Beschreibung und Informationen
TaintDroid	Privacy Monitoring; Ansatz: Taint Tracking: http://www.appanalysis.org/faq.html Nicht im Playstore Hinweis: AntiTaintDroid http://gsbabil.github.io/AntiTaintDroid/
DroidBox	Verwendet taintDroid für Taint Tracking und führt VMI (mit Dalvik VM patch) durch Verwendbar über Desktop/Android SDK https://www.honeynet.org/gsoc2011/slot5 https://code.google.com/archive/p/droidbox/
Mobile Sandbox	Ansatz: VMI und System Call Monitoring (SCM) Aus Mobworm-Projekt: https://www.syssec.rub.de/research/completed/MobWorm/ https://www.syssec.rub.de/research/publications/Mobile-Sandbox/
SmartDroid	Ansatz: Method Call Analyse, http://faculty.cse.tamu.edu/guofei/paper/SmartDroid-SPSM12.pdf
ANANAS	Logt Filesystem-Aktivität, Netzwerkaktivität und Systemaufrufe , API Monitoring
DroidScope	VMI und Taint Tracking mit TaintTracker (eig Implementierung)
Andrubis	VMI, Event-Monitoring, System call Monitoring, verwendet TaintDroid
TraceDroid	
CopperDroid	
SandDroid	
VisualThreat	
Joe Mobile APK Analyzer	
Badger	
AndroTotal	

6.2 Manifest-Datei (Beispiel)

```
<?xml version="1.0" encoding="utf-8"?>
<manifest
  xmlns:android="http://schemas.android.com/apk/res/android"
  package="de.einefirma.beispiel"
  android:versionCode="3"
  android:versionName="1.2" >

  <uses-sdk android:minSdkVersion="8" android:targetSdkVersion="23" />
```

```
  <uses-permission android:name="android.permission.INTERNET" />

  <application android:allowBackup="true"
    android:icon="@drawable/ic_launcher"
    android:label="@string/app_name"
    android:theme="@style/AppTheme" >

    <activity android:name="de.einefirma.beispiel.main_activity"
      android:label="@string/title_activity_main" >

      <intent-filter>
        <action   android:name="android.intent.action.MAIN />
        <category android:name="android.intent.category.LAUNCHER" />
      </intent-filter>

    </activity>

    <activity android:name="de.einefirma.beispiel.hilfe_activity"
      android:label="@string/title_activity_hilfe" >
    </activity>

  </application>

</manifest>
```

(Entnommen aus https://www.droidwiki.de/Manifest.)

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="com.example.myapplication">

    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE" />
    <uses-permission android:name="android.permission.READ_INTERNAL_STORAGE" />
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />

    <application
        android:allowBackup="true"
```

KIT Scientific Working Papers
ISSN 2194-1629

www.kit.edu