Wer weiß was? – Digitale Privatsphäre und App-Literacy aus Nutzerperspektive

Christoph Buck [1], Daniela Kaubisch[2] und Torsten Eymann[1]

[1] Universität Bayreuth, Lehrstuhl für Wirtschaftsinformatik, vorname.nachname@unibayreuth.de
[2] Universität Bayreuth, Lehrstuhl für Wirtschaftsinformatik, wi@unibayreuth.de

Abstract

Der zügellose Konsum mobiler Applikationen wird in der Literatur unter anderem mit theoretischen Konstrukten wie dem Privatsphäre-Paradox erklärt. Da diese theoretische Grundlage die Perspektive der Nutzer und deren spezifische Vorbildung vollkommen außer Acht lässt, adressiert der Artikel die App-Literacy der Nutzer um zu ergründen, ob sich Nutzer im Umgang mit Privatsphäre paradox verhalten. Anhand einer qualitativen empirischen Studie wird die spezifische Bildung der Nutzer bestimmt und anhand einer Inhaltsanalyse gezeigt, dass die Nutzer die durch mobile Applikationen drohenden Privatsphäre-Gefahren aufgrund ihrer zu niedrigen App-Literacy nicht einschätzen können und sich somit nicht paradox verhalten. Der Artikel zeigt, dass Nutzer Angebote mobiler digitaler Ökosysteme zwar ausgiebig in Anspruch nehmen, die daraus entstehenden Gefahren jedoch nicht kennen und somit auch nicht einschätzen und bewerten können.

1 Einleitung

„Privatsphäre sollte nicht nur eine Wahl sein, die wir treffen können, und sie sollte sicherlich nicht der Preis sein, den wir bezahlen müssen, nur um im Internet surfen zu dürfen.“ (Kovacs 2012)

Smartphones sind heutzutage als Alltagsbegleiter von Konsumenten kaum mehr wegzudenken und gehören zu der meist verkauften elektronischen Geräteklasse. Smartphones stellen dabei einen umfassenden Speicherort von Erinnerungen, Inhalten, Interessen und Verhalten dar und versetzen Datenaggregatoren in die Lage ein Abbild des realen Lebens des Konsumenten und des (gewünschten) Selbstbildes des Nutzers zu erstellen. Es existiert folglich ein stetig wachsendes Archiv an verifizierten und personalisierten Informationen mit höchster Datengüte, das auf ein Smartphone eindeutig zurückverfolgt werden kann (Egele et al. 2011). Anders als Computer, Laptops oder Tablets kann ein Smartphone als personalisiertes Endgerät angesehen werden, wodurch das umfassende Datenarchiv über die Geräte-Identifikator (ID) und das Nutzerprofil des Operating System (OS)-Anbieters einem Nutzer eindeutig zugeordnet werden kann. Durch die unzähligen Möglichkeiten der Sammlung, Speicherung und Verarbeitung von persönlichen Informationen ergeben sich für Nutzer massive Gefahrenpotentiale durch Verletzungen ihrer Privatsphäre (Enck 2011).

Insbesondere das Geschäftsmodell von kostenlos verfügbaren mobilen Applikationen (Apps) basiert auf der Sammlung und Auswertung von persönlichen Daten. Obwohl den meisten Nutzern das Bezahlen mit persönlichen Daten bewusst sein müsste, beziehen sie scheinbar bedenkenlos verschiedenste Apps auf ihr Smartphone. Dieses paradoxe Verhalten wird in der Literatur als Privatsphäre-Paradoxon bezeichnet (Norberg et al. 2007), (Jensen et al. 2005). Das Privatsphäre-Paradox unterstellt, dass sich Nutzer paradox in Bezug auf mobile Applikationen (Apps) verhalten: Sie lehnen Anwendungen, welche persönliche Daten (weiter-)verwenden, im Allgemeinen ab, verhalten sich aber im Speziellen entgegengesetzt (Wenninger et al. 2012).

Der vorliegende Artikel versucht die Hintergründe des vermeintlich paradoxen Verhaltens von Nutzern zu ergründen und strebt eine weiterführende Erklärung des Phänomens des ungezügelten App-Konsums an. Die hierbei zugrunde liegende Hypothese besagt, dass Nutzer, welche eine nur eingeschränkte spezifische Bildung (Literacy) hinsichtlich Privatsphäre-Gefahren (Art und Umfang der Datenaufnahme, -aggregation und -verarbeitung) besitzen, sich aufgrund der bestehenden Informationsasymmetrie nicht paradox verhalten. Dementsprechend verfolgt der Artikel die Beantwortung der beiden folgenden Forschungsfragen:

- Verfügen private Nutzer über App-Literacy und reicht diese aus um Privatsphäre-Gefahren im mobilen Ökosystem zu erkennen und einschätzen bzw. bewerten zu können?

Im nachfolgenden Kapitel wird die relevante Literatur zu digitaler Privatsphäre und Privacy-Literacy diskutiert, die Besonderheiten digitaler mobiler Ökosysteme dargestellt und Diskrepanzen zwischen Privatsphäre-Bedenken und Handeln erläutert. In Kapitel 3 wird die qualitative empirische Studie zur Untersuchung der Privacy-Literacy vorgestellt. Der Artikel schließt mit einer Schlussbetrachtung, den Limitationen der Studie und möglichen zukünftigen Forschungs-richtungen.

2 Theoretische Grundlagen

2.1 Relevante Literatur zur Privatsphäre und App-Literacy

Das Konstrukt Privatsphäre ist in mehrdimensionaler Weise komplex und kann aus unterschiedlichen Blickwinkeln betrachtet werden (Hotter 2011).[1] Eine der wohl bekanntesten Definitionen stammt von Warren und Brandeis und definiert Privatsphäre als "the right to be let alone" (Warren und Brandeis 1890). Diese Worterklärung ist jedoch sehr allgemein und unvollständig, da sie in Bezug auf persönliche Daten und deren Preisgabe den überaus wichtigen Bestandteil der Kontrolle außer Acht lässt (Bok 1983). Rössler (2001) bedenkt zudem, dass nicht immer das kontrolliert werden kann, was kontrolliert werden sollte, wie z.B. die Weitergabe von Daten an Dritte. Im Folgenden wird der Begriff nach Hotter (2011, 83) verstanden als ein

„Schutzmechanismus, der dem Individuum durch die Möglichkeit des selektiven Verbergens und Veröffentlichens der eigenen Person individuelle Freiheit garantieren soll“.[2]

[1] So gibt es beispielsweise soziologische, philosophische, psychologische, rechtliche, anthropologische, feministische und politische Ansätze. Zusätzlich hat sich der Begriff bzw. die Annahme darüber, was privat ist, im Zeitverlauf gewandelt [He11].

[2] Welche Bedeutung Privatsphäre für ein Individuum hat, wird oftmals unterschätzt. Rössler (2001) stellt dazu die These auf, dass eine autonome Lebensführung nur möglich unter Bedingungen geschützter Privatsphäre ist. Eingriffe in die Privatsphäre sind deshalb auch immer Verletzungen der Bedingungen von Autonomie. In liberalen Gesellschaften gilt es jedoch zu beachten, dass die Privatsphäre nur ein relativer Wert sein kann, da diese durch die Freiheiten anderer Mitbürger, wie z.B. der Pressefreiheit oder der freien Meinungsäußerung, begrenzt ist und die Intensität der Privatsphäre auch von den eigenen Eigentumsverhältnissen abhängt.

Durch die neuen Medien und Informationstechnologien werden Individuen immer mehr zu gläsernen Konsumenten, wodurch der Schutz der Privatsphäre gefährdet ist.

Personenbezogene Informationen haben demnach zunehmend den Charakter einer Ressource bzw. eines Tauschobjekts. Oftmals ist der Verzicht auf die Kontrolle der persönlichen Daten Bedingung für die Nutzung von digitalen (Öko-)Systemen, wodurch die Verantwortung auf private Vertragspartner übergeht und Nutzer eine unübersichtliche Vielzahl einzelner Verträge mit Privaten Vertragspartnern einzugehen haben. Diese Entwicklung stellt nicht nur eine Gefahr der Privatsphäre dar, sondern auch eine Gefahr für ein selbstbestimmtes, autonomes Leben und individuelle Freiheit, da eine selektive Selbstveröffentlichung und Verschließung innerhalb digitaler Freiheitsspielräume nur bedingt kontrollierbar ist (Hotter 2011).

Ob und inwiefern sich Nutzer über derartige Gefahren und Gefahrenpotentiale bewusst sind, bzw. bewusst sein können ist die Messung deren App-Literacy (Buck et al. 2014). In Analogie zum Begriff Digital Literacy, der nach Park (2014) die Vertrautheit mit den technischen Aspekten des Internets, die Kenntnis über institutionelle Gewohnheiten und gängige Privatsphäre-Praktiken umfasst, wird der Begriff App-Literacy hier im Kontext mobiler Applikationen eingesetzt. In der Literatur bestehen weitere Begriffe wie Privacy Awareness, Computer Literacy oder Privacy Literacy, die jedoch nicht mit dem hier beschriebenen Begriff App Literacy synonym verwendet werden können. Besonders der Begriff Privacy Literacy mag sehr zutreffend klingen, wird jedoch bereits schon von Vegheş et al. (2012) als die Einstellung der Nutzer bezüglich der Sammlung, Nutzung und Verarbeitung ihrer persönlichen Daten beschrieben. Vegheş et al. (2012) lassen somit das technische Know-how der Nutzer außer Acht. Der Begriff App Literacy hingegen beschreibt den Kenntnisstand und die Vertrautheit von Nutzern über die technische Funktionsweise von mobilen Applikationen und die Bildung der Nutzer im Hinblick auf Privatsphäre-Gefahren, was ebenfalls ein Verständnis über die Funktionsweise des App-Marktes einschließt. Ein Nutzer mit geringer App Literacy kann beispielsweise potentielle Privatsphäre-Gefahren nicht adäquat erkennen, da ihm dazu die zugrundeliegenden spezifischen Kenntnisse fehlen. Ein Nutzer mit hohem App Literacy versteht dagegen die zugrundeliegende Funktionsweise und Praxis mobiler Applikationen und kann Gefahren besser erkennen und dementsprechend zielgerichteter handeln.

Innerhalb der Forschungsdomäne des Information Systems Management (IS) können nur wenige Arbeiten identifiziert werden, die Literacy direkt oder indirekt untersuchen. Liao et al. (2011), Furnell und Moore (2014), Kraus et al. (2014) und Malhotra et al. (2004) ziehen die Literacy der Nutzer als erklärende Variable hinzu, allerdings steht Literacy nicht im Zentrum der Untersuchungen. Eine Vielzahl anderer Studien untersuchen zudem die Literacy der Nutzer bezüglich des Mediums Internet (Hargittai 2005), (Yamakami 2012). Eine Übertragbarkeit auf den mobilen Kontext ist aufgrund der Besonderheit des mobilen Ökosystems nur sehr begrenzt möglich. Einzig die Studie von Kraus et al. (2014) untersucht die App-Literacy im mobilen Kontext. Kraus et al. (2014) untersuchen dabei Privatsphäre und Sicherheitskenntnisse (P&S-Kenntnisse) und Privatsphäre-Bedenken als Prädiktor für Nutzung bzw. Nichtnutzung von Schutzmechanismen.

2.2 IT-Sicherheit in mobilen digitalen Ökosystemen

Das mobile Ökosystem weist im Vergleich zur webbasierten Systemarchitektur zwei hauptsächliche Besonderheiten auf, die zum einen den Aspekt der Datensammlung und zum anderen die technischen Beschränkungen des mobilen Ökosystems umfassen. Diese Besonderheiten werden im Folgenden eingehender betrachtet, bevor ein Einblick in die Sicherheitsthematik beim Design der mobilen Applikationen gegeben wird.

Die erste Besonderheit besteht darin, dass bei der Nutzung von Apps validierte und hochgradig personalisierte Datensätze über den Nutzer gewonnen werden können (Buck et al. 2014). Durch die Kumulation der gesammelten spezifischen Informationen einzelner Apps kann eine bisher nicht erreichbare Datenaggregation stattfinden. Anders als bei web-based Services, wie beispielsweise Facebook oder Twitter, sind bei der Autorisierung von Apps über das Betriebssystem zusätzliche, für Manipulationen nicht anfällige, validierte Daten, wie MAC-Adresse, Geräte-ID, Telefonnummer und hinterlegte Kontoinformationen für In-App Bezahlmethoden verfügbar (Buck et al. 2014).

Die zweite Besonderheit besteht beim Smartphone im Vergleich zum PC darin, dass Smartphones viel geringere Rechenleistungen aufweisen und deshalb auch nur abgespeckte Sicherheitssysteme integrieren. So haben Smartphones keine ausgetüftelte Firewall, keine intelligenten Detektions- und Abwehrmechanismen bei Systemangriffen und auch kaum eine effektive physische Zugangskontrolle (Posegga und Schreckling 2011). Zudem kommt, dass bei mobilen Netzwerken im Vergleich zum wired Netzwerk die offene Übertragung drahtloser Signale, die hohe Fehlerrate bei der drahtlosen Übertragung sowie das Sicherheitsmanagement für das Smartphone und die Sicherheitsbedenken beim Aufzeichnen der Aufenthaltsorte problematischer sind. Durch die Möglichkeiten der umfassenden Datenaggregation ist die Anforderung an eine sichere Systemarchitektur im mobilen Umfeld höher, jedoch sind gleichzeitig mehrere technische Restriktionen zu beachten, die einen Aufbau eines sicheren Systems sehr schwierig gestalten. Es sind beispielweise komplexe Codes als Verschlüsselungsverfahren oder manche Sicherheits-Netzwerkprotokolle, wie beispielsweise Webservices, im mobilen Umfeld nicht oder nur schwer einsetzbar, da eine hohe Rechenleistung oder eine stabile Internetverbindung benötigt werden, die in mobilen Systemen nicht immer gegeben ist (Theng und Li 2006).

2.3 Diskrepanz zwischen Privatsphäre-Bedenken und Handeln

Aufgrund der zahlreichen Privatsphäre-Gefahren auf den verschiedenen Infrastrukturebenen, den zahlreichen Akteuren im Datensammlungs- und Verarbeitungsprozess, der Besonderheit der App-Systemarchitektur und den komplizierten und oftmals unzureichenden Datenschutzbestimmungen, sollte ein rationaler Nutzer erhebliche Privatsphäre-Bedenken beim App-Download aufweisen.

Privatsphäre-Bedenken sollen hier nach der Definition von Dinev und Hart (2006) und Xu et al. (2012) als Bedenken um den möglichen zukünftigen Verlust der Privatsphäre als Folge von freiwilliger oder unfreiwilliger Preisgabe von sensiblen Daten bezeichnet werden. Privatsphäre-Bedenken resultieren dabei aus der digitalen Kommunikation und Transaktion mit teilweise anonymen Akteuren, der Intransparenz des zugrunde liegenden App-Marktes und aus der Nutzung und Interaktion mit Apps, was von den Nutzern einen gewissen Kenntnisstand zur Bedienung und Nutzung von Apps abverlangt (Liao et al. 2011).

Es bleibt unklar, ob Nutzer überhaupt in der Lage sind, sicherheitsrelevante Entscheidungen vernünftig treffen zu können und adäquate Sicherheitskontrollen durchzuführen (Mylonas et al. 2013). So sind Nutzer meist recht gut darin, einzelne Risiken aufzuzählen, weil sie etwa in den Medien thematisiert werden (Friestad und Wright 1994), (Campbell und Kirmani 2000). Jedoch fehlt es ihnen an Grundverständnis, um zu erklären, warum und in welchem Kontext bestimmte Risiken ernst genommen werden sollten (Vedder 2011). Dies stellt Nutzer beim App-Downloadprozess und -Nutzungsprozess auf die Probe, da eine gewisse App-Literacy verlangt wird, um beurteilen zu können, welche App-Berechtigungen Privatsphäre-Risiken bergen. Meist werden die Berechtigungen bestätigt, da oftmals weitere Details der Berechtigungen das Know-

how des Nutzers übersteigen (Posegga und Schreckling 2011). Aufgrund dieses Wissens- und Informationsdefizits des Nutzers ist der App-Markt durch das Vorliegen asymmetrischer Informationen gekennzeichnet, welche von den App-Nutzern nur durch erhebliche Transaktionskosten, wie beispielsweise durch das Aneignen eines technischen Verständnisses, überwunden werden können. Eine geringe App-Literacy kann Privatsphäre-Bedenken und den Handlungsspielraum der Nutzer beeinflussen, da zur Entscheidungsfindung beim App-Kauf essentielle Informationen vorliegen, aber nicht verstanden werden.

Sollten die Nutzer tatsächlich eine sehr geringe App-Literacy aufweisen, dann beruhen die Risikoabwägungen, wie sie beispielsweise beim Privacy-Calculus-Erklärungsansatz von Dinev und Hart (2006) getätigt werden, auf falschen Annahmen und verzerren die Risiko-Nutzenabwägung im erheblichen Maße. Gleichzeitig ruhen Privatsphäre-Bedenken auf Risiko-Wahrnehmungen und der Faktor Vertrauen könnte je nach App-Literacy variieren. Die Vermutung liegt also nahe, dass eine Korrelation zwischen App-Literacy und den anderen Erklärungsvariablen vorliegt. Eine genaue Untersuchung zur App-Literacy von Nutzern ist daher essentiell, um in der Lage zu sein, ein theoriegestütztes Model zur Erklärung des Privatsphäre-Paradoxes aufstellen zu können.

3 Qualitative Studie zur App-Literacy

3.1 Methodik der qualitativen Studie

Für die vorliegende Studie wurde ein teilstandardisiertes Leitfadeninterview angewendet, da diese Methode zwei positive Ansätze miteinander verbindet. Zum einem helfen offene Fragen beim Eingrenzen des interessierenden Problembereichs und sorgen für einen erzählenden Stimuli (Lamnek 2010), bei denen die Befragten die Möglichkeit haben, den Detaillierungsgrad selbst zu bestimmen. Zum anderen wird dem Interviewer durch die vorgegebenen Themen ein Rahmen geboten, in dem er sich bewegen kann. Das Vorwissen des Forschers dient dabei zur Strukturierung des Interviewleitfadens.

Die Auswertung des Datenmaterials wurde mit Hilfe der qualitativen Inhaltsanalyse vorgenommen (Mayring 2008). Beim diesem Analyseverfahren werden die erhobenen Daten ausgewertet, indem inhaltlich unveränderte Aussagen zu Kategorien zusammengefasst werden und das Datenmaterial auf diesem Wege reduziert wird (Mayring 2008).[3]

Im Rahmen der Auswertung der vorliegenden Studie fand eine Orientierung an der inhaltlich strukturierten qualitativen Inhaltsanalyse nach Kuckartz (2014) statt, da sie ein exploratives Vorgehen ermöglicht und nicht verfrüht zu Bewertungen drängt, wie dies etwa bei evaluativen oder typisierenden Inhaltsanalysen der Fall ist. Die Kategorien werden hierbei in einem mehrstufigen Verfahren gebildet. In der ersten Stufe wird eine Kategorisierung entlang der Hauptkategorien des Leitfadens vorgenommen, anschließend werden weitere Kategorien am Material weiterentwickelt und ausdifferenziert. Die kategorienbasierte Auswertung und Darstellung gewinnt somit an Differenziertheit, Erklärungskraft und Komplexität.

[3] Die Spezifika dieses Verfahren sind durch ein systematisches Verfahren nach expliziten Regeln gegeben, sodass eine intersubjektive Nachprüfbarkeit gewährleistet werden kann. Aus dem theoriegeleiteten Annahmen und dem empirischen Material werden schließlich Kategorien gebildet (Mayring 2008).

3.2 Datenerhebung und Aufbereitung

Relevant für die Studie sind Personen, die Smartphones und Applikationen nutzen, weshalb die Nichtnutzung einer der beiden Services Ausschlusskriterien darstellen. Eine bestimmte Altersgrenze wurde nicht gesetzt, da jeder Smartphone-User mit der Privatsphäre-Problematik gleichermaßen konfrontiert ist. Um eine gezielte Manipulation zu vermeiden, wurden nicht nur Personen zum Interview gebeten, von welchen bekannt ist, dass sie im Umgang mit Applikationen ein bestimmtes Bildungsniveau aufweisen. Die Auswahl der Befragten wurde entsprechend nach leicht erreichbaren, motivierten und verfügbaren Personen getroffen, weshalb die Befragten aus dem sozialen Umfeld der Autoren stammen. Die Autoren haben dabei versucht, die Auswahl nach sozialen und demografischen Faktoren zu glätten.

Insgesamt wurden 23 Personen befragt, welche die definierten Auswahlkriterien erfüllten und zudem ihr Einverständnis zur Aufzeichnung und Auswertung der im Rahmen des Interviews erhobenen Daten in anonymisierter Form erklärten. Unter ihnen sind 13 Teilnehmer weiblich, 10 von ihnen sind männlich. Die Altersgruppe reicht von 13 bis 60 Jahren, wobei das Durchschnittsalter rund 31,52 Jahre und der Median 26 Jahre beträgt. 65% der Befragten haben einen Hochschulabschluss, 17% ein Abitur, 13% einen Realschulabschluss und 4% keinen Schulabschluss. Die größte Gruppe unter den Befragten stellen die Berufstätigen mit ca. 52,2% dar, gefolgt von Studierenden (30,4%), Personen in Ausbildung (8,7%), Schülern und Arbeitslosen (jeweils 4,3%).

Die darauf folgende Inhaltsanalyse wurde mit Hilfe der Computersoftware MAXQDA11 durchgeführt. Die Durchführung der Datenauswertung erfolgte nach der inhaltlich strukturierenden qualitativen Inhaltsanalyse nach Kuckartz (2014).

3.3 Ergebnisse

Auf Basis der systematischen Kodierung des Datenmaterials wurde die in Tabelle 1 bereit gestellte Themenmatrix erarbeitet, die es erlaubt kategorienbasierte und fallbezogene Aussagen zu machen[4].

Bei den beiden Hauptkategorien zu den Kenntnissen über das App-Geschäftsmodell und über die technische Funktionsweise von Apps wurde nach diesem Schema vorgegangen. Bei der Hauptkategorie zur Datensammlung wurde zusätzlich zu den Subkategorien eine Zusammenfassung auf allgemeiner Ebene vorgenommen, da nur diese Ebene aufzeigen konnte, wie viele der Interviewer durch Nachfragen an zusätzlichen Antworten erhalten konnte. Da diese Nachfragen vielen Befragten weitere Anhaltspunkte gaben, konnten von ihnen deutlich mehr Informationen erfragt werden.[5] Erst durch Nachfragen konnten zusätzliche Angaben gesammelt werden. Dadurch ist eine Zusammenfassung auch auf allgemeiner Ebene der Hauptkategorie in diesem Falle sinnvoll, da nur dadurch ein reelles und umfassendes Abbild über die Kenntnisse zur Datensammlung aufgezeigt werden kann.

[4] Jede Textpassage der Matrix kann dabei auf das Originalmaterial der mittels MAXQDA codierten Textpassage zurückverfolgt werden.
[5] Bspw. bei Probanden, welche über Art und Umfang der potentiellen Datensammlung keinerlei Kenntnis besaßen.

Themenmatrix					
	Hauptkategorie 1		Hauptkategorie 2		
	Subkategorie	Subkategorie	Subkategorie	Subkategorie	→Fallzusammenfassung
Interview 1	Textstellen	Textstellen	Textstellen	Textstellen	→Fallzusammenfassung
Interview 2	Textstellen	Textstellen	Textstellen	Textstellen	→Fallzusammenfassung
Interview 3	Textstellen	Textstellen	Textstellen	Textstellen	
	Kategorienbasierte Auswertung ↓	↓	↓	↓	
	Thema 1.1	Thema 1.2	Thema 2.1	Thema 2.2	

Tabelle 1: Themenmatrix, in Anlehnung an Kuckartz (2014)

Das Wissen der Nutzer über die Datensammlung von ortsbasierten Angaben ist sehr hoch. Ganze 20 von 23 Befragten sind sich darüber bewusst, dass Apps ihre Standorte, bis hin zu Aufenthaltsmustern, aufzeichnen können. Des Weiteren sind sich viele Nutzer auch bewusst, welche ihrer gängigen Apps ihre Standorte aufzeichnen.

Die Kenntnisse der Nutzer über die Aufzeichnung personenbezogener Daten können als mittelmäßig eingestuft werden. Fast die Hälfe der Befragten wissen, dass Angaben zur Person, wie beispielsweise dem Alter, Wohnort und Geschlecht, von Apps erhoben werden können. Knapp die Hälfte der Befragten ist sich zudem darüber bewusst, dass auch E-Mail-Adressen von Apps gesammelt werden können. 10 von 23 Befragten überblicken, dass auch ihre Fotos gesammelt werden können. Nur 2 von 23 Befragten sind sich darüber bewusst, dass ebenso ihre Passwörter von Apps gesammelt werden können.

Das Wissen über indirekt ermittelbare Daten ist sehr gering. Nur wenige Nutzer sind sich darüber bewusst, dass Apps Daten über Interessen, Konsummuster, Suchanfragen, Haushaltseinkommen oder das Alltagsverhalten sammeln. 21,7% der Befragten wissen, dass Daten über ihr Shopping-Verhalten oder ihre Shopping-Interessen aufgezeichnet werden. Die meisten Nutzer geben in diesem Zusammenhang an, dass sie dieses anhand der ihnen zugestellten und zugeschnittenen Werbung erkennen. Rund 17,4% der Befragten ist bewusst, dass ihre allgemeinen Suchanfragen über das mobile Internet aufgezeichnet werden. Nur 2 von 23 Befragten wissen, dass auch ihr Haushaltseinkommen, ihr komplettes Konsummuster, ihre Daten über ihr soziales Umfeld und ihre Beziehungen zu Kontakten aus der Kontaktliste aufgezeichnet werden können. Des Weiteren sind sich ebenfalls nur 2 von 23 Befragten darüber im Klaren, dass die Nutzungsaktivität, welche Auskunft über den Alltagsrhythmus geben kann, ebenfalls von Apps gesammelt werden kann.

Die Kenntnisse über das App-Geschäftsmodell sind gering, da die gesetzlichen Regelungen meist unbekannt sind. Nur wenige Probanden wissen über den vollen Umfang des App-Geschäftsmodells Bescheid. Sie gehen davon aus, dass Daten (Suchverläufe) gesammelt werden, um personalisierte Werbung zuzusenden oder anzuzeigen. Dass jedoch Apps aus dem Nutzerverhalten der Anwender weitaus detailliertere Erkenntnisse über diese ziehen können, ist den meisten Befragten nicht bewusst.

Das Wissen über gesetzliche Datenschutzbestimmungen ist sehr unterschiedlich ausgeprägt. 6 von 23 Befragten scheinen komplett ahnungslos zu sein. Sie hoffen, dass ihre Daten sicher aufbewahrt werden und eine Weitergabe an Dritte nicht möglich ist. Mehr als ein Drittel der Befragten (8 von 23) wusste oder vermutete, dass mit dem Download die Nutzungsberechtigungen akzeptiert werden, in welchen stehen könnte, dass die Daten weitergegeben werden können. Mehr als ein Viertel der Befragten (6 von 23) ist jedoch der Meinung, dass in den Nutzungsberechtigungen steht, dass Daten eben nicht weitergegeben werden können. Die wenigsten Nutzer lesen sich die Nutzungsberechtigungen durch, viele wissen aber, dass dort die Datenschutzrichtlinien stehen müssten. Als Grund für das Nichtlesen der Nutzungsberechtigungen geben die Meisten an, dass diese ihnen zu lang und zu unverständlich sind.

Eine geringe Anzahl (3 von 23) vermutet, dass App-Betreiber die Daten illegal weitergeben. Nur ein Sechstel der Befragten gibt an, dass es darüber hinaus entscheidend ist, welches Datenschutzgesetz Anwendung findet und verweist auf nationale Unterschiede. Nur ein Befragter, ein Jurist, konnte sagen, dass das ausländische Recht meist etwas lockerer ist und deshalb die Datenweitergabe einfacher umzusetzen wäre. Auffällig ist jedoch bei allen Befragten, dass sie sich mit diesem Thema zuvor noch nicht auseinandergesetzt haben und deshalb relativ unsicher sind.

Auch die Kenntnisse über die Weitergabe der Daten weichen stark voneinander ab. 40% der Befragten geben an, dass die Daten eigentlich nicht weitergegeben werden, wobei zwei Drittel dieser Befragten (also 6 von 9) angeben, dass sie davon ausgehen, dass die Daten grundsätzlich nicht weitergeben werden. Ein Drittel dieser Befragten (also 3 von 9) gehen davon aus, dass die Daten grundsätzlich nicht weitergegeben werden, es sei denn der App-Betreiber tut dies illegal oder am Rande des Gesetzes.

Viele der Befragten gehen somit fälschlicherweise davon aus, dass ihre Daten nicht weitergeben werden dürfen, da sie sonst hätten zustimmen müssen. Dass sie dieser Weitergabe wahrscheinlich schon oft durch das Akzeptieren der Nutzungsbestimmungen erlaubt haben, ist ihnen nicht bewusst. Auch Hinweise des Interviewers auf die Nutzungsberechtigungen helfen den Befragten nicht.

Nur knapp die Hälfte der Befragten (11 von 23) besitzen Kenntnis über die Weitergabe der Daten an Dritte. Die restlichen Befragten wissen nicht, ob Daten weitergegeben werden.

Die Kenntnis über die Datenaggregation ist sehr gering. Bei der Nutzung von Apps haben nur äußerst wenige App-Nutzer ein aktives Bewusstsein darüber, dass ihre Daten zu Nutzerprofilen aggregiert werden können. Vielen Nutzern fällt auf, dass die Datensammlung dazu dient, dem Nutzer Werbung zuzuschicken. Allerdings berichten die meisten Befragten dies im Zusammenhang mit Suchanfragen z.B. bei Google über das mobile Internet. Dass auch das Verhalten der Nutzer resultierend aus der App-Nutzung für solche Werbe- und Marktforschungszwecke erhoben wird, ist vielen Befragten nicht bewusst. Zudem haben nur zwei Befragte angemerkt, dass datenverarbeitende Unternehmen Daten einzelner Apps aggregieren. Wie dieser Prozess aber konkret ablaufen könnte, scheinen die Befragten nicht zu wissen.

Eine große Anzahl der Befragten nennt aber den Datenaustausch zwischen Apps in Zusammenhang mit dem Login über einen Identity Provider. Einem Großteil der Nutzer ist hierbei bewusst, dass sie dadurch mehr Daten an z.B. Facebook oder der jeweiligen App freigeben. Grund für eine Missempfindung über diese Verschmelzung von Identity Provider und App ist oftmals Unbehagen darüber, dass die App auf der eigenen Chronik Inhalte posten könnte und dass somit Facebook oder die jeweilige App noch mehr Daten sammeln könnte.

Das technische Wissen über die Funktionsweise von Applikationen der Nutzer weicht sehr stark voneinander ab. Während die Kenntnisse über Privatsphäre-Risiken auf Hardware-Ebene zufriedenstellend sind, fehlt es Nutzern oftmals an grundlegenden Kenntnissen über die Privatsphäre-Risiken auf der Software-Ebene. Bei den Privatsphäre-Risiken auf Netzwerk-Ebene zeigt sich, dass die Befragten ein Basisverständnis aufweisen, wobei es ihnen an spezifischen Wissen fehlt, um fallbezogen Risiken eigenständig erkennen zu können. Anzumerken ist hierbei, dass einige Befragte mit geringer App-Literacy sich nicht auf ihr eigenes Wissen berufen, sondern Entscheidungen in Absprache mit Freunden oder Bekannten mit vermeintlich hoher App-Literacy treffen.

Die Befragten zeigen fast alle Kenntnisse über die Privatsphäre-Risiken auf Netzwerk- Ebene, die einem Basis-Level zugeschrieben werden können. Beinahe alle Befragten wissen, dass Privatsphäre-Risiken auf der Netzwerk-Ebene existieren. Den meisten Befragten (19 von 23) ist bewusst, dass ihre Daten auf Netzwerkebene abgefangen werden können. Wird allerdings nachgefragt, wie bspw. Hacker detailliert an die Daten kommen oder in welchen Situationen Nutzer besonders gefährdet sind, sind die Meisten sehr unwissend.

Nur 5 von 23 Personen haben Kenntnisse darüber, dass ihre Daten bei der Nutzung öffentlicher Netzwerke leichter abzufangen sind. Nur 2 Befragte geben an, dass Hacker auch Passwörter abfangen könnten. Über den Datendiebstahl durch Hacker auf Host-Ebene, falls Apps Daten in einer Cloud gespeichert sind, berichten 5 von 23 Befragten. Es gehen rund 74% der Befragten davon aus, dass nicht alle Apps Daten verschlüsselt übertragen. Insgesamt sind die meisten Befragten sich aber bewusst, dass die Übertragung nicht sicher ist und gehen vorsichtiger mit der Preisgabe sensibler Informationen um.

Die Kenntnisse der Nutzer über die Privatsphäre-Risiken auf Hardware Ebene sind recht gut. Die persönlichen Risiken im Falle eines Gerätediebstahls variieren mit den installierten Apps und dem Umgang mit vertraulichen Informationen. Da in der Studie sehr unterschiedliche Nutzertypen vorliegen, ist die Beurteilung über die Kenntnis zu Privatsphäre-Risiken fallbezogen. Dennoch lässt sich festhalten, dass die meisten Nutzer wissen, dass Fremde direkten Zugang auf Apps haben, sollte der Dieb die Sperre umgehen können. Zudem sehen die Meisten Risiken darin, dass der Dieb in deren Namen Inhalte an ihre Facebook-Freunde oder E-Mail-Kontakte schicken könnte.

Nur eine geringe Anzahl der Befragten ist sich darüber im Klaren, dass der Dieb auch herausfinden könnte, wann eine Person im Urlaub ist und somit die Wohnung etc. frei ist. Zudem wissen Einige, dass der Dieb Käufe z.B. über iTunes, App Stores oder In-App-Käufe tätigen könnte und somit einen finanziellen Schaden auslösen könnte. Manchen ist darüber hinaus auch bewusst, dass Daten nicht nur aus Apps genutzt werden können, sondern auch von Browserseiten, auf welchen der Nutzer automatisch eingeloggt ist und Passwörter hinterlegt hat. Hierbei handelt es sich auch teilweise um Shopping-Seiten.

Die Kenntnisse über die Privatsphäre-Risiken auf Software-Ebene sind sehr gering. Rund 70% der Befragten fehlen Kenntnisse darüber, ob App Stores Apps auf Malware überprüfen. 75% von diesen haben keine Ahnung von Prüfprozessen, die übrigen 25% gehen von falschen Annahmen aus und geben an, dass der App Store Apps auf Malware überprüft. Nur ein Nutzer mit einem iOS Betriebssystem gibt an, dass der App Store Apps auf Malware überprüft, was richtig ist, und wurde dementsprechend nicht der beschriebenen Gruppe zugeordnet. Ca. 30% der Befragten (7/23) sind somit in der Lage, eine korrekte Antwort zu geben. Davon geben 6 der 23 befragten Android-Nutzer an, dass Apps nicht auf Malware überprüft werden.

Die Kenntnisse zu den App-Berechtigungen sind ähnlich gering. Werden die Nutzer gefragt, was unter der App-Berechtigung "Geräte-ID und Anrufinformationen" zu verstehen ist, geben die Meisten gleich an, dass sie das nicht wüssten. Erst durch Nachhaken, versuchen sich die Befragten die Antwort zusammenzureimen, sodass letztendlich 15 Android-Nutzer die richtige Antwort wussten oder diese zumindest vermuteten. Unter Anrufinformationen können sich viele Nutzer jedoch nichts vorstellen. Diejenigen, die mit dem Begriff " Geräte-ID" etwas anfangen konnten, wissen nicht, warum App-Betreiber diese Informationen sammeln. 4 von 15 Befragten gehen davon aus, dass App-betreiber diese Herstellerinformationen brauche, um zu überprüfen, ob die App auf ihrer Geräteklasse funktioniert. Nur 2 von 15 Befragten ist bewusst, dass die ID u.a. für die eindeutige Zuordnung zu Nutzerprofilen erhoben wird.

4 Schlussbetrachtung, Limitationen und zukünftige Forschung

Der vorliegende Artikel nähert sich der Thematik der App-Literacy über eine qualitative empirische Studie. Aufgrund ihres explorativen Charakters und ihrer qualitativen Ausrichtung weist die Studie zahlreiche Limitationen auf. Diese sind bspw. in der Möglichkeit sozial erwünschter Antworten, der Repräsentativität der Stichprobe und der Selbstselektion der Teilnehmer zu sehen. Aufgrund ihres explorativen Charakters um sich dem Themenfeld der App-Literacy zu näher ist die Arbeit vorwiegend deskriptiver Natur und zielt auf die Reproduzierung des Wissensstands der App-Nutzer ab. Die Generalisierbarkeit der Studienergebnisse wird durch die Auswahl der Probanden eingeschränkt. Detaillierte Angaben zum Umfang und Art der Nutzung und der genutzten Apps können hinsichtlich der Probanden nicht gemacht werden.

Trotz dem explorativen Charakter erlaubt die Studie einen Rückschluss bezüglich der aufgeworfenen Forschungsfragen. Nutzer von Apps und mobilen digitalen Ökosystemen verfügen zwar über eine geringe (Basis-)App-Literacy, diese reicht jedoch nicht aus um Privatsphäre-Gefahren erkennen und einordnen zu können. Trotz der massiven Nutzung mobiler digitaler Ökosysteme und deren App-Angebote durch Drittanbieter scheinen die Nutzer die hieraus entstehenden mittel- und langfristigen Gefahren nicht einschätzen zu können. Vor diesem Hintergrund scheint es fraglich, ob Nutzer überhaupt in der Lage sind, Privatsphäre-Risiken im beschriebenen Kontext richtig einzuschätzen. Eine niedrige App-Literacy kann eine weitere Erklärungsvariable für das aus der Literatur bekannte Privacy Paradox liefern. So kann ein möglicher Erklärungsmehrwert aus der Argumentation heraus entstehen, dass Nutzer mobiler Applikationen Ihre Selbstverantwortung des Abbaus vorhandener Informationsasymmetrien auf andere Parteien (bspw. App-Provider, App-Store-Betreiber) auslagern. Forschungsarbeiten im Rahmen des Privacy Paradox und der Verhaltensökonomie stützen diese Erkenntnisse, beispielweise durch verschiedene Heuristiken (Acquisti et al. 2015; Brandimarte et al. 2013). Eine niedrige App-Literacy kann somit eine Erklärung für die Argumentation und theoretische Grundlage des Privacy Paradox liefern und verlangt nach massiven Maßnahmen im Hinblick auf Schutz, Prävention und Aufklärung von App-Nutzern.

Zukünftige Forschungsvorhaben sollten somit verstärkt auf die spezifische Bildung von Nutzern digitaler Systeme eingehen um die tatsächlich vorhandenen Kosten-Nutzen-Abwägungen beschreiben zu können. Die qualitativen Ansätze zur Untersuchung der App-Literacy sollten weitergeführt und in ein valides quantitatives Konstrukt zu einer generalisierbaren App- und Privacy-Literacy überführt werden.

5 Literatur

Acquisti, A, Brandimarte, L, Loewenstein, G (2015) Privacy and human behavior in the age of information. In: Science 347(6221): 509-514

Brandimarte, L, Acquisti, A, Loewenstein G (2013) Misplaced confidences privacy and the control paradox. In: Social Psychological and Personality Science 4(3), 340-347

Buck C, Horbel C, Kessler T, Germelmann CC (2014) Mobile Consumer Apps: Big Data Brother is Watching You. In: Marketing Review St. Gallen 31(1):26–34

Bok S (1983) Secrets: On the ethics of concealment and revelation. New York: Pantheon Books (3)

Campbell M, Kirmani A (2000) Consumers' Use of Persuasion Knowledge: The Effects of Accessibility and Cognitive Capacity on Perceptions of an Influence Agent. In: Journal of Consumer Research 27(1):69-83

Dinev T, Hart P (2006) An Extended Privacy Calculus Model for E-Commerce Transactions. In: Information Systems Research 17(1):61–80

Egele M, Kruegely C, Kirda E, Vigna G (2011) PiOS: Detecting Privacy Leaks in iOS Applications. http://www.cs.ucsb.edu/~chris/research/doc/ndss11_pios.pdf. Abgerufen am 28.08.2015.

Enck W (2011) Defending Users against Smartphone Apps: Techniques and Future Directions. In: Hutchison, D. et al. (Hrsg.) Information Systems Security, Lecture Notes in Computer Science, 7093, Springer Berlin Heidelberg

Friestad M, Wright P (1994) The Persuasion Knowledge Model: How People Cope with Persuasion Attempts. Journal of Consumer Research 21(1):1-31

Furnell S, Moore L (2014) Security literacy: the missing link in today's online society? In: Computer Fraud & Security (5):12–18

Hargittai E (2005) Survey Measures of Web-Oriented Digital Literacy. In: Social Science Computer Review 23(3):371–379

Hotter M (2011) Privatsphäre. Der Wandel eines liberalen Rechts im Zeitalter des Internets. Frankfurt am Main [u.a.]: (951) Campus-Verlag

Kovacs G (2012) Beobachten wir die Beobachter. Übersetzt von Mario Wagner. TED. http://www.ted.com/talks/gary_kovacs_tracking_the_trackers/transcript?language=de. Abgerufen am 28.08.2015.

Kraus L, Wechsung I, Möller S (2014) A Comparison of Privacy and Security Knowledge and Privacy Concern as Influencing Factors for Mobile Protection Behavior. In: Contribution to the Workshop on Privacy Personas and Segmentation (PPS) at the Symposium on Usable Privacy and Security (SOUPS). http://cups.cs.cmu.edu/soups/2014/workshops/privacy/s2p4.pdf. Abgerufen am 28.08.2015.

Kuckartz U (2014) Qualitative Inhaltsanalyse. Methoden, Praxis, Computerunterstützung. 2 Auflage. Beltz Juventa, Weinheim

Lamnek S (2010) Qualitative Sozialforschung. Lehrbuch. 5. Auflage. Beltz Verlag, Weinheim

Liao C, Liu C, Chen K (2011) Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model. In: Electronic Commerce Research and Applications 10(6):702-715.

Mayring P (2008) Qualitative Inhaltsanalyse. Grundlagen und Techniken. 10. Auflage. Beltz Verlag, Weinheim

Malhotra NK, Kim SS, Agarwal J (2004) Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale and the Casual Model. In: Information Systems Research 15(4):336–355

Mylonas A, Kastania A, Gritzalis D (2013) Delegate the smartphone user? Security awareness in smartphone platforms. In: Computers & Security 34(0):47–66

Norberg PA, Horne DR, Horne DA (2007) The privacy paradox: personal information disclo-sure intentions versus behaviors. Journal of Consumer Affairs 41, 100–126

Park YJ (2014) Digital Literacy and Privacy Behavior Online. In: Communication Research (40):215–236

Posegga J, Schreckling D (2011) Next Generation Mobile Application Security. In: U. Bub (Hrsg.) IT-Sicherheit zwischen Regulierung und Innovation. Tagungsband zur zweiten EICT-Konferenz IT-Sicherheit. 1. Auflage. Vieweg+Teubner Verlag (IT-Sicherheit und Datenschutz), Wiesbaden

Rössler B (2001) Der Wert des Privaten. 1. Auflage. Suhrkamp Verlag (Suhrkamp Taschenbuch Wissenschaft, 1530), Frankfurt am Main

Theng P, Li L (2006) Smart-Phone and Next-Generation Mobile Computing. Morgan & Kaufman Publishers, San Francisco

Vedder A (2011) Privacy 3.0. In: van der Hof, S. und M. M. Groothuis (Hg.) Innovating Government, Bd. 20. The Hague, The Netherlands: T. M. C. Asser Press (Information Technology and Law Series)

Vegheş C, Orzan M, Acatrinei C, Dugulan D (2012) Privacy Literacy: What is it and how it can be measured? In: Annales Universitatis Apulensis Series Oeconomica 14(2):704–711. http://www.oeconomica.uab.ro/upload/lucrari/1420122/36.pdf. Abgerufen am 28.08.2015.

Warren SD, Brandeis LD (1890) The Right to Privacy. In: Harvard Law Review 1890, 05.12.1890 (5):1–37. http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html. Abgerufen am 28.08.2015.

Wenninger H, Widjaja T, Buxmann B, Gerlach J (2012) Der "Preis des Kostenlosen". Wirtschaftsinformatik & Management 3(6):2–18

Xu H, Rosson MB, Gupta S, Caroll, JM (2012) Measuring Mobile User's Privacy Concerns for Information Privacy. In: Thirty Third International Conference on Information Systems

Yamakami, T (2012) Digital Social Literacy: Literacy Demands for the Virtual-World. In: Rachid Benlamri (Hrsg.) Networked Digital Technologies, Bd. 294. Springer Berlin Heidelberg (Communications in Computer and Information Science), Berlin