Methoden zur Schaffung von Bewusstsein über persönliche Informationen als notwendige Voraussetzung für den Schutz der Privatsphäre

Von der Fakultät für Elektrotechnik und Informatik
der Gottfried Wilhelm Leibniz Universität Hannover
zur Erlangung des akademischen Grades eines

Doktor der Naturwissenschaften
Dr. rer. nat.

genehmigte Dissertation

von

M. Sc. Benjamin Henne
geboren am 03.08.1981
in Hannover

2014

Referent: Prof. Dr. rer. nat. Matthew Smith
Korreferentin: Prof. Dr.-Ing. Gabriele von Voigt

Tag der Promotion: 2014/09/04

Danksagung

Für die Unterstützung beim Erstellen dieser Arbeit, insbesondere für die Unterstützung meiner Forschungsarbeiten, die die Basis für diese Dissertation bildeten, und das entgegengebrachte Vertrauen bedanke ich mich besonders bei Herrn Professor Matthew Smith. Außerdem gilt mein Dank Frau Professorin Gabriele von Voigt, die immer ein offenes Ohr für mich hatte.

Meinen Kollegen aus der Distributed Computing & Security Group danke ich für die anregenden Diskussionen zu den von mir verfolgten Forschungsarbeiten sowie für die gute Zusammenarbeit an gemeinsamen Themen. Darüber hinaus bedanke ich mich bei meinen langjährigen Kollegen für die vertrauensvolle und persönliche Arbeitsatmosphäre.

Ebenfalls bedanke ich mich bei allen Studierenden, die im Rahmen von Abschlussarbeiten, Projektarbeiten in der Lehre und als studentische und wissenschaftliche Hilfskräfte bei Implementierungen und zum Teil bei der Durchführung von Studien mitgewirkt haben. Insbesondere danke ich dabei Marcel Linke, Philipp Tute, Christian Kater und Maximilian Koch für die gute Zusammenarbeit.

Herzlich bedanke ich mich bei meiner Mo, die mir beim Entstehen dieser Arbeit zur Seite gestanden hat. Sie hat mich stets motiviert, mir Rückhalt gegeben und mich mit ihrer Rücksichtnahme und Geduld unterstützt.

Ebenfalls danke ich meinen Eltern herzlich für den Zuspruch und den gegebenen Rückhalt in den vergangenen Jahren.

Hannover, im Juni 2014

Zusammenfassung

Im Rahmen der Nutzung von IT-Systemen geben die Menschen heute häufig persönliche Informationen preis, die zu einer Bedrohung ihrer Privatsphäre führen können. Früher gaben vor allem die Überwachung und die Profilerstellung durch Anbieter Anlass zur Sorge. Seit einigen Jahren werden jedoch Unmengen an persönlichen Informationen von den Nutzern selbst preisgegeben, indem diese Inhalte im Web teilen und kontextsensitive Dienste nutzen. Nach einem anfänglichen Preisgabe-Rausch ist mittlerweile vielen Menschen klar geworden, dass das übermäßige Teilen von Inhalten und das Teilen mit unpassendem Publikum für Probleme sorgen können. Um in diesem Fall Bedrohungen ihrer Privatsphäre zu vermeiden, können die Nutzer ihr Verhalten anpassen, da sie wissentlich eigene Daten teilen, die sie unter ihrer Kontrolle haben. Problematisch ist jedoch, wenn ihnen die Kontrolle über preisgegebenen Informationen fehlt und weitaus schwerwiegender noch, wenn den Nutzern nicht bewusst ist, dass Informationen durch sie selbst oder Andere preisgegeben werden.

Das Bewusstsein über persönliche und personenbezogene Informationen ist eine notwendige Voraussetzung zum Schutz der Privatsphäre. Erst mit dem Wissen über die Existenz von Informationen kann ein Nutzer entscheiden, ob diese Teil seiner privaten Sphäre sind oder ob sie Teil der öffentlichen Sphäre werden dürfen, um schließlich die Preisgabe entsprechend zu kontrollieren. Diese Dissertation betrachtet die Problematik des Fehlens von Bewusstsein über persönliche Informationen, das die Nutzer daran hindert, ihre Privatsphäre zu wahren. Neben einer allgemeinen Betrachtung des identifizierten Problems untersucht diese Arbeit das Fehlen von Bewusstsein anhand zweier Anwendungsfälle im Detail. Es werden Methoden vorgestellt und evaluiert, die in den jeweiligen Anwendungsfällen Bewusstsein schaffen können, um die Privatsphäre der Betroffenen besser zu schützen.

Im Kontext des Social Webs wird das Bewusstsein der Nutzer über geteilte Fotos betrachtet, welche die Privatsphäre der Nutzer betreffen können. Insbesondere werden Bilder betrachtet, die Andere teilen. Studienergebnisse zeigen das momentan vorhandene Bewusstsein der Nutzer und motivieren Bewusstsein schaffende Maßnahmen. Es werden verschiedene Methoden vorgestellt, die das fehlende Bewusstsein über relevante Bilder anderer Nutzer verringern können. Da Bild-Metadaten auch Bedrohungen herbeiführen können, werden diese ebenfalls betrachtet. Es wird gezeigt, wie ausgeprägt die Verwendung von Metadaten heute ist. Um Bewusstsein über die häufig nicht sichtbaren Informationen zu schaffen, wird eine Methode präsentiert, die Metadaten geteilter Bilder visualisiert. Während des Teilens schafft sie zudem Bewusstsein über eingebettete Metadaten und ermöglicht deren Kontrolle.

Im Kontext mobiler Geräte wird die Nutzung kontextsensitiver Dienste betrachtet. Es wird eine Methode vorgestellt, die Bewusstsein über preisgegebene Standortinformationen schafft. Sie ermöglicht Nutzern darüber hinaus den Detailgrad preisgegebener Informationen zu kontrollieren, um Standortinformationen zu verwenden und gleichzeitig die Privatsphäre der Nutzer bestmöglich zu schützen.

Exemplarisch erfassen die vorgestellten Methoden verschiedene Aspekte des Bewusstseins über persönliche Informationen: die Preisgabe durch Andere, die Existenz verborgener Daten und deren implizite Mitpreisgabe und die gewollte Preisgabe durch die Nutzer.

Schlagwörter: Privatsphäre, nutzerfreudlicher Privatsphäreschutz, Bewusstsein, Social Media, Fotos, Metadaten, mobile Apps, Standortinformationen, Standortverschleierung

Abstract

When using modern information technology, people often expose personal information potentially causing threats to their privacy. Previously, user tracking and the creation of user profiles by third parties were the main sources of privacy concerns. However, today much more information is voluntarily revealed by the users themselves, as they share content on Web or use context-based services. After a period of massively sharing personal information, many people have begun to realize that oversharing and sharing with the wrong audience may cause problems. To mitigate this threat to their privacy, users can opt to rationally change their behavior, since they consciously share their own data, which is under their control. However, the preservation of privacy becomes difficult if people are not able to exercise control over the data. Problems become even worse if the users are not aware of the fact that certain information is being revealed by themselves or others at all.

Awareness of personal information is a necessary requirement for the protection of user privacy. Only users who are aware of the existence of certain information can decide whether that information belongs to their private sphere or whether it may become part of the public sphere, and finally exercise the desired control over it. This dissertation explores the problem of unawareness of personal information that prevents users from preserving their privacy. Besides a general description of the identified problem, this work in detail explores the lack of awareness about personal information within two fields of application. As part of the investigation, different measures are proposed and evaluated that aim to raise awareness about personal information in the respective applications to facilitate privacy preservation.

In the context of the social Web users' awareness of shared photos that may be relevant for their privacy is surveyed. In particular, photos shared by other people are considered. The results of user studies reveal users' actual awareness and motivate measures that are needed to improve awareness. Different measures are then presented, aiming to reduce the prevalent unawareness of relevant images taken or uploaded by others. Since image metadata also could cause threats to privacy, it is considered as well. Image analysis shows how widespread the use of metadata is today. A measure is presented that raises awareness of the commonly non-visible information. It visualizes metadata of shared images. Additionally, it creates awareness and allows for control over embedded metadata in the moment of sharing.

In the context of mobile devices the use of context-based services is addressed. A measure is introduced that raises awareness of disclosed location information. It additionally allows users to control the level of detail of disclosed information. This enables the use of location data while at the same time it best possibly protects users' privacy.

The proposed measures exemplarily cover different aspects of the awareness about personal information: the disclosure by others, the existence of hidden information and its implicit revelation, as well as the conscious disclosure by the users.

Keywords: privacy, usable privacy, awareness, social media, photos, metadata, mobile apps, location information, location obfuscation

Inhaltsverzeichnis

Abkürzungsverzeichnis

ACM	Association for Computing Machinery
AJAX	Asynchronous JavaScript and XML
API	Application Programming Interface
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
DC	Dublin Core
DCSec	Distributed Computing & Security
DNG	Digital Negative
DOI	Digital Object Identifier
EGNOS	European Geostationary Navigation Overlay Service
Exif	Exchangeable Image File Format
GG	Grundgesetz
GLONASS	Global Navigation Satellite System
GNSS	Globales Navigationssatellitensystem
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
IIM	Information Interchange Model
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
IPTC	International Press Telecommunications Council
ISO	International Organization for Standardization
IT	Informationstechnik
JFIF	JPEG File Interchange Format
JPEG	Joint Photographic Experts Group
LBPH	Local Binary Patterns Histograms
LNCS	Lecture Notes in Computer Science
MAC	Media Access Control

MAD ..... Mittlere absolute Abweichung vom Median
MWG ..... Metadata Working Group
NAA ..... Newspaper Association of America
NFC ..... Near Field Communication
NISO ..... National Information Standards Organization
P3P ..... Platform for Privacy Preferences
PDA ..... Personal Digital Assistant
PDF ..... Portable Document Format
PHP ..... PHP: Hypertext Preprocessor
PNG ..... Portable Network Graphics
RDF ..... Resource Description Framework
RRZN ..... Regionales Rechenzentrum für Niedersachsen
SQL ..... Structured Query Language
SSH ..... Secure Shell
SSL ..... Secure Socket Layer
SUS ..... System Usability Scale
TIFF ..... Tagged Image File Format
TOR ..... The Onion Router
URI ..... Uniform Resource Identifier
URL ..... Uniform Resource Locator
UTM ..... Universal Transverse Mercator
WGS-84 ..... World Geodetic System 1984
WLAN ..... Wireless Local Area Network
WWW ..... World Wide Web
XML ..... Extensible Markup Language
XMP ..... Extensible Metadata Platform

Kapitel 1

Einleitung

Seit rund 20 Jahren durchlebt die Menschheit einen rasanten Wandel der Technik. Die Entwicklung des Internets und des Webs verdeutlicht die Geschwindigkeit:

Das World Wide Web entstand vor etwa 20 Jahren als Teil des Internets. Für Laien wurde der Zugang zum weltweiten Informationsnetzwerk kurz darauf durch die Veröffentlichung der ersten grafischen Webbrowser ermöglicht. Heute, nur 20 Jahre später, besitzt über die Hälfte der Bewohner von Industriestaaten wie Deutschland, Großbritannien oder den USA ein mobiles Gerät, welches den Zugang zum Web und dem Internet von fast überall aus ermöglicht [4, 31, 34]. Und mit der Vision des Internets der Dinge vor Augen schreitet die Entwicklung weiter voran: Mehr und mehr Gebrauchsgegenstände von Autos bis hin zu Küchenutensilien werden miteinander und mit dem Internet verbunden.

Die Computerisierung von Beruf und Freizeit, die Digitalisierung von Informationen und die moderne Kommunikation haben in den vergangenen Jahren einen deutlichen Einfluss auf viele Lebensbereiche der Menschen genommen. Neben dem Berufsleben hat die Informationstechnik heute auch das Private und das soziale Lebensumfeld der Menschen durchdrungen. Heute ersetzt vielerorts das Online-Banking den Kontakt zum Bankangestellten, eingekauft wird im Web, Geburtstagseinladungen erhalten die Online-Freunde im Sozialen Onlinenetzwerk, statt Passanten fragen viele ihr Smartphone nach dem Weg oder nach dem nächstgelegenen Café und viele Teilen ihr Leben mit anderen online statt bei einem persönlichen Zusammentreffen.

Die Vielfalt und die Komplexität des Ökosystems der Informationstechnik nehmen stetig zu und die Technik durchdringt immer wieder neue Lebensbereiche. Der positive Nutzen vieler Neuerungen sorgt für eine schnelle Adaption, nicht mehr nur durch Technikliebhaber, sondern häufig durch die breite Masse. Die Komplexität von Geräten und Software stellt jedoch für viele Nutzer eine Herausforderung dar.

Obwohl die heutige Technik und insbesondere die eingesetzte Software den Zugang und die Nutzung oftmals erleichtern, kann die Komplexität der Systeme nicht immer vollständig vor den Nutzern verborgen werden. Andersherum kann gerade

die Vereinfachung des Zugangs zur Technik und das Verbergen der technischen Details auch Probleme entstehen lassen. Der vereinfachte Zugang erlaubt mehr Laien die Nutzung der Informationstechnik und schafft eine breitere jedoch auch unerfahrenere Nutzerbasis. Die Abstraktion von Details erleichtert den Umgang, jedoch minimiert sie auch das Wissen über zugrunde liegende Technologien und technische Details, welches für ein umfassendes Verständnis oft notwendig wäre. Neben diversen Problemen im Umgang mit der Technik entstehen so insbesondere auch Bedrohungen der Privatsphäre oder der IT-Sicherheit, weil die Nutzer zugrunde liegende Probleme oft nicht verstehen. Schlimmer noch, sie kennen die Gründe oder Auslöser häufig gar nicht. Es ist Aufgabe der Forschung und Entwicklung dieses Problem zu lösen.

1.1 Motivation

Viele Bereiche des alltäglichen Lebens sind heute mit Informationstechnik (IT) durchsetzt. Ein Großteil der Menschen kommuniziert heutzutage mobil und über das Internet. Die Menschen fotografieren mit Digitalkameras oder Kamera-Handys. Das Buch aus Papier wird immer öfter durch einen E-Book-Reader ersetzt und viele hören statt Radio ihre persönliche Musiksammlung vom MP3-Player.

Um neben den Basisfunktionen weitere Komfortfunktionen bieten zu können, integrieren viele Geräte und Anwendungen internetbasierte Funktionen. Angebunden über drahtlose Netzwerke oder das Mobilfunknetz visualisieren moderne Kameras den Ort eines Fotos auf einer Karte, E-Book-Lesezeichen wandern unbemerkt auf andere Geräte eines Nutzers und fehlt einmal ein Buch oder ein Musikstück, so wird es automatisch über das Internet bezogen. Für viele Menschen ist es heute normal allzeit erreichbar zu sein und auch allzeit online sein zu können: für das Lesen und Schreiben von Nachrichten, eine Suche im Web oder um neue Eindrücke mit anderen über das Internet oder im Web zu teilen. Durch die vielseitige Integration von Online-Angeboten ist das Internet, meist in Form des Webs oder mobiler Anwendungen, für viele Menschen fester Bestandteil des alltäglichen Lebens geworden.

Nicht nur die Technik, sondern auch die Rolle der Nutzer hat sich dabei über die Jahre verändert. Aus Informationskonsumenten, die Webseiten betrachteten oder im Web einkauften, wurden ab der Jahrtausendwende Prosumenten: Im Web 2.0 produzieren die Nutzer nun ebenso Inhalte wie sie sie konsumieren, beispielsweise durch Beiträge in Wikis, in persönlichen Blogs oder in themenfokussierten Online-Communitys. Mit der Weiterentwicklung des Webs entstanden schließlich Soziale Onlinenetzwerke wie Facebook und diverse Formen von Social Media. Die Menschen nutzen diese Dienste heute zum kollaborativen Arbeiten, für das Knüpfen und Wahren sozialer Kontakte und für die soziale Interaktion mit anderen wie dem Austausch von Informationen und dem Teilen von Texten, Fotos oder Videos.

Nutzung in Zahlen

Laut der ARD/ZDF-Onlinestudie 2013 [1] nutzen 77,2 % der Deutschen ab 14 Jahren das Internet an 5,8 Tagen mit einer durchschnittlichen täglichen Nutzungsdauer von 169 Minuten. Eine Erhebung des Statistischen Bundesamtes über das Jahr 2012 bestätigt die Nutzerzahl: 77 % der Befragten gaben an, das Internet täglich oder fast jeden Tag zu nutzen [41]. In Großbritannien ist die Nutzung ähnlich hoch: 73 % der Erwachsenen nutzten im Jahr 2013 das Internet täglich [31]. Hingegen sind in den USA die Zahlen sogar höher: Im Jahr 2013 griffen 85 % der Erwachsenen und 2012 97 % der Jugendlichen (12 bis 17 Jahre) auf das Internet zu [35, 33]. Innerhalb Deutschlands ist die durchschnittliche Internet-Nutzung in der Gruppe der Jugendlichen und jungen Erwachsenen (14 bis 29 Jahre) mit 218 Minuten am höchsten und die Nutzungsdauer von Besitzern mobiler Geräte ist mit 208 Minuten an 6,3 Tagen überdurchschnittlich hoch [1].

Mobile Geräte wie Smartphones oder Tablets haben zuletzt besonders zur beschriebenen Entwicklung beigetragen. Sie erleichtern den Zugang durch eine einfache Bedienung. Ihre Multifunktionalität wie auch ihre Mobilität und die Möglichkeit des spontanen Zugriffs sorgen für einen vielseitigen und häufigen Einsatz. Allein 2013 wurden laut BITKOM auf dem deutschen Markt 26,4 Millionen Smartphones und 8 Millionen Tablets abgesetzt, während es im Vorjahr 21,6 und 5 Millionen waren [3].

Im ersten Quartal des Jahres 2012 nutzten 85 % der Deutschen ein Mobiltelefon [41] von denen laut ComScore [4] zu diesem Zeitpunkt rund 40 % ein Smartphone verwendeten. Bis Juli 2013 stieg der Anteil der Smartphone-Nutzer auf 59 % aller Mobiltelefonbesitzer. Eine Erhebung der Tomorrow Focus AG [49] ergab, dass 73,4 % der Befragten das Internet über ein Mobiltelefon täglich nutzen. Während eine Studie der Forsa/Accenture [15] dies mit einem Wert von 70 % bestätigt, wirkt das Ergebnis der ARD/ZDF-Onlinestudie 2013 [1] einschränkend: Die Studie ergab, dass 41 % der Internetnutzer das Internet außerhalb von Wohnung und Arbeitsplatz nutzen, während es im Vorjahr nur 23 % waren. Zum Vergleich, im Jahr 2013 nutzten in Großbritannien 53 % der Erwachsenen das Internet über ein Mobiltelefon [31] und in den USA nutzten 63 % der Mobiltelefonbesitzer das Internet über ihr Telefon [36].

IT-Sicherheit und Privatsphäre

Mit der allgegenwärtigen Nutzung von Informationstechnik und Internet-Angeboten ist auch die IT-Sicherheit und Privatsphäre ein allgegenwärtiges Thema geworden. Allzeit online zu sein bedeutet, allzeit potenziellen IT-Gefahren ausgesetzt zu sein. Spielte die IT-Sicherheit schon seit den frühen Jahren der IT eine Rolle, so wurde sie doch oft stiefmütterlich behandelt. Durch die heutige breite Adaption der Technik rückt sie jedoch immer weiter in den Fokus der Dienstanbieter und vieler Nutzer. So soll beispielsweise niemand das zwischen Geräten geteilte Adressbuch unerlaubt

lesen oder unbemerkt verändern dürfen oder sich unter falschem Namen kostenlosen Zugang zu einem Buch oder Musikstück verschaffen können. Während dies jedoch klassische Sicherheitsszenarien sind, hat sich besonders durch den Wandel der Rolle der Nutzer von Konsumenten zu Prosumenten und der massiven Verbreitung und Adaption von Online-Communitys, Sozialen Onlinenetzwerken und nutzerkontextsensitiven Diensten die Privatsphäre der Nutzer zu einem besonders schutzbedürftigen Gut entwickelt.

Schon seit den Anfängen des Webs war der Schutz der Privatsphäre der Nutzer gegenüber Anbietern, die Daten über Nutzer beim Surfen oder Online-Einkauf sammelten, ein grundlegendes Thema. Mit der Verbreitung von Web-2.0-Angeboten und sozialer Interaktion über das Web ist die Bedrohung der Privatsphäre für die Nutzer jedoch massiv gestiegen. Die Nutzer geben nun von sich aus persönliche Informationen preis. Sie teilen persönliche Daten wie auch Bilder und Videos nicht nur mit einem Dienstanbieter, sondern mit anderen Nutzern, oft beschränkt auf einen kleineren Personenkreis, jedoch auch weltöffentlich. Eine weitere Quelle für Bedrohungen der Privatsphäre stellen nutzerkontextsensitive Dienste dar. Sie bieten Nutzern Informationen oder Funktionen, die auf ihren persönlichen Informationen basieren. Sowohl in Form von Webangeboten als auch durch Anwendungen auf mobilen Geräten werden Dienste angeboten, die Nutzern beispielsweise das nächstgelegene Café zeigen, eine Mitfahrgelegenheit vorschlagen oder neue Musik empfehlen.

Die Preisgabe von Informationen stellt sich heute im Rahmen des Web 2.0, des Social Webs und kontextsensitiver Dienste oft mehr als komplexer Konflikt dar und nicht wie zuvor als persönliche Grundsatzentscheidung im Sinne von „dafür oder nicht“. Die Anbieter sind in der Pflicht mit ihren Diensten das jeweils geltende Recht zum Schutz personenbezogener Daten einzuhalten. Sie haben jedoch das ureigene Interesse an den personenbezogenen Informationen der Nutzer: Neben der Profilerstellung oder der personalisierten Werbung dienen die Informationen der Verbesserung des Angebots, um Nutzer zu gewinnen oder zu halten. Je mehr Informationen zur Verfügung stehen, desto individueller und genauer können viele Funktionen angeboten werden. Je mehr persönliche Informationen ein Nutzer preisgibt, desto eher lässt er andere in seine Privatsphäre eindringen. Folglich haben Nutzer hingegen das ureigene Interesse Informationen über sich selbst so gut es geht zu schützen. Je mehr ein Nutzer jedoch preisgibt, desto mehr Funktionen kann er nutzen. Die Entscheidung für eine Funktion kann persönliche Informationen an einen Anbieter preisgeben. Die konsequente Entscheidung für die Privatsphäre schließt hingegen die Nutzung mancher Funktionen aus. So muss ein Nutzer des Android-Betriebssystems bis dato den Zugriff auf bestimmte Informationen tolerieren, wenn er eine Anwendung installieren und nutzen möchte. Die Meidung Sozialer Onlinenetzwerke, die von persönlichen Informationen leben, kann manchmal den Kontakt zu Freunden erschweren, so dass sogar soziale Konflikte durch den Wunsch nach Privatsphäre entstehen können.

Problembeschreibung

Grundsätzlich gilt: Bei der Nutzung von IT-Diensten sollen die Nutzer selbst entscheiden können, welche Informationen Teil der eigenen privaten Sphäre sind und welche Teil der öffentlichen Sphäre werden. Dies gilt unabhängig davon, ob ein Nutzer Informationen nur mit einem Anbieter teilt, sie weltöffentlich präsentiert oder sie durch Zugriffskontrollen eines Dienstes nur einem beschränkten Personenkreis zugänglich macht. Problematisch wird die Wahrung der Privatsphäre jedoch, wenn Nutzern nicht bewusst ist, wann und wo sie selbst mit persönlichen Informationen agieren, jemand anderes mit ihren Informationen agiert oder ein von ihnen verwendeter Dienst dies tut. Ebenso problematisch ist es, wenn sich die Nutzer nicht über das Vorhandensein persönlicher Informationen in „harmlosen“ Daten bewusst sind. Das Wissen um die Existenz verborgener Informationen ist ein notwendiges Kriterium, um zu entscheiden, ob die gesamten Daten privat oder öffentlich sind. Den Nutzern muss bewusst sein, welche Informationen mit welchem Detailgrad verwendet werden, um die Nutzung oder den Detailgrad beschränken zu können.

Hier kommen deutliche Nebenwirkungen der rasanten und vielfältigen Entwicklung und des vereinfachten Zugangs zur Technik zum Vorschein. Ein Großteil der Nutzer hat kein ausreichendes Wissen über technische Hintergründe und verwendete Informationen, welches notwendig wäre, um Bedrohungen der eigenen Privatsphäre zu erkennen. Selbst wenn sie ihre Privatsphäre schützen wollen, sind sich viele Nutzer einer Vielzahl potenzieller Bedrohungen nicht bewusst. Die Ursache für das Fehlen von Wissen oder Bewusstsein ist dabei jedoch nur zu Teilen bei den Nutzern zu suchen, denn die Technik selbst trägt ihren Teil dazu bei: Die einfach zu benutzende Technik sorgt dafür, dass die Nutzer sich nur wenig mit technischen Details auseinandersetzen. Des Weiteren bietet die heutige Technik selbst interessierten Nutzern häufig nur beschränkte Einblicke in ihre Privatsphäre betreffende Details. Dies ist teils auf die schwierige Darstellung in Nutzerschnittstellen und auf deren Komplexität zurückzuführen, es scheint teils jedoch auch schlichtweg gewollt zu sein.

In der Praxis können das fehlende Bewusstsein und die persönlichen Informationen viele Facetten haben: Ein Nutzer weiß beispielsweise nicht, welche nicht direkt sichtbaren Zusatzinformationen in einer Datei gespeichert sind und mit ihr verbreitet werden. Ein anderer hingegen weiß nicht, welche Anwendung auf seinem Smartphone zu welchem Zeitpunkt auf seinen via GPS- oder WLAN-basierter Ortsbestimmung ermittelten aktuellen Aufenthaltsort zugreift.

Bei der Bedrohung der eigenen Privatsphäre durch die Preisgabe persönlicher Informationen spielen heute klar ersichtlich auch andere Faktoren eine Rolle: beispielsweise das Desinteresse oder eine hohe Gelassenheit gegenüber der eigenen Privatsphäre oder das deutliche Überwiegen des Gewinns einer gebotenen Funktionalität im Vergleich zum als geringer angesehenen Verlust gewisser privater Informationen.

Auch bei diesen eher persönlich oder gesellschaftlich geprägten Faktoren spielt das Bewusstsein über preisgegebene Informationen eine Rolle, denn ohne Kenntnis über das Preisgegebene kann eine Entscheidung auch auf einer Fehleinschätzung beruhen.

Ein weiterer Aspekt des fehlenden Bewusstseins ist die Auswirkung des Handels auf andere: Oft können preisgegebene Informationen auch andere Personen betreffen und im Umkehrschluss kann die Privatsphäre eines Nutzers durch das Handeln anderer unwissentlich beeinträchtigt werden. Das fehlende Bewusstsein kann somit auf beider Seiten liegen. Unbewusst und unbeabsichtigt kann jemand ein fragliches Bild im Web teilen, in dem der Name eines Dritten enthalten ist. Oder ein Nutzer weiß nicht, wo im Web ihn betreffende Informationen, Fotos oder Videos veröffentlicht wurden. In der aktiven Rolle des Teilenden müssen die Nutzer auch wissen, wann und wo sie mit persönlichen Informationen Anderer agieren, um verantwortlich handeln zu können. Außen vor bleibt dabei natürlich die Frage, ob sie sich für die Privatsphäre Anderer verantwortlich fühlen, unabhängig von der Ausgestaltung ihrer eigenen. In der passiven Rolle der Betroffenen haben die Nutzer bisher kaum Möglichkeiten sich über Informationen bewusst zu werden, die Andere über sie preisgeben.

Das Fehlen von Bewusstsein über die Preisgabe persönlicher Informationen als Ursache für die Bedrohung der Privatsphäre ist ein Problem, welches sich über einen Großteil der heutigen Informationstechnik erstreckt. Von besonderer Kritikalität sind die Fälle, in denen momentan die Zahl der Nutzer und die Zahl potenzieller Bedrohungen besonders rasant wachsen. Zwei Fälle dieser Art werden im Rahmen dieser Dissertation genauer betrachtet: geteilte Fotos im Social Web und standortbezogene Funktionen mobiler Geräte.

1.1.1 Geteilte Fotos im Social Web

Die Veröffentlichung von Bildmaterial ist schon seit über 100 Jahren ein Punkt für Streitigkeiten um Bildrechte und die Privatsphäre abgebildeter Personen. Schon im Jahr 1898 verschafften sich zwei Fotografen Zugang zum Sterbezimmer des ehemaligen Reichskanzlers Otto von Bismarcks. Ihre Fotografien des Verstorbenen sorgten für einen Presseskandal noch vor einer juristischen Verankerung des Rechts am eigenen Bild [73]. Ebenso gab es schon 10 Jahre zuvor in den Vereinigten Staaten von Amerika diverse Auseinandersetzungen über Fotos von Privatpersonen oder Personen in der Öffentlichkeit wie beispielsweise die unerlaubte Fotografie einer Broadway-Darstellerin, die für eine Theaterrolle in Strumpfhosen aufgetreten war [147].

Dennoch war die Einhaltung von Bildrechten und die Wahrung des Rechts am eigenen Bild lange Zeit vorwiegend ein Problem von Journalisten und Fotografen sowie von abgelichteten Personen des öffentlichen Lebens. Der Großteil der Privatfotografie beschränkte sich lange darauf, Fotos und Dias zuhause zu sammeln und mit Freunden und Bekannten gemeinsam zu betrachten. Mit Rechtsvorschriften kamen

Privatpersonen wohl meist nur in Berührung, wenn sie beispielsweise als Fotograf an einem Fotowettbewerb teilnahmen oder in seltenen Fällen Teil eines öffentlich dargestellten Bildes waren. Es gab kaum eine Bedrohung der Privatsphäre durch private Bilder solange diese daheim in Fotoalben und Diakästen verwahrt wurden.

Innerhalb der letzten 10 bis 20 Jahre hat sich jedoch mit dem technischen Wandel Grundlegendes an der Situation geändert, so dass die Veröffentlichung von Bildern zu einem Massenproblem geworden ist. Vor rund 20 Jahren kamen die ersten Digitalkameras auf den Massenmarkt und begannen damit die Fotografie zu verändern. Circa 10 Jahre später überboten die Verkaufszahlen von Digitalkameras die der analogen Kameras und Kamera-Handys kamen vermehrt auf den Markt. Auch wenn die Auflösung und der Speicherplatz der Geräte anfangs begrenzt waren, konnten von da an viele Fotos geschossen werden, ohne Aufwand und laufende Kosten durch Filme und Entwicklung zu erzeugen. Günstige Speicherkarten mit großem Speichervolumen bewirkten letztendlich, dass heute fast ohne Grenzen fotografiert werden kann. Seit ein paar Jahren sind Kameras durch das eigene Mobiltelefon oder in Form kleiner Kompaktkameras in sehr vielen Lebenslagen dabei, was zu einer Vielzahl spontaner und unüberlegter Fotos führt. Die heute erreichte Auflösung der Geräte zeichnet dabei sogar Personen im Hintergrund meist deutlich erkennbar auf.

Etwa zeitgleich mit der anfänglichen Verbreitung von Digitalkameras erlaubten Freehoster bereits in den ersten Jahren des World Wide Webs das Hochladen und weböffentliche Darstellen von Bildern im Rahmen privater Webseiten. Mit der Entstehung von Online-Communitys zum Hochladen und Kommentieren von Fotos wurde dies vor etwa 10 Jahren professionalisiert. Mit der Entstehung von Diensten wie Photobucket, Picasa und Flickr [26] war so der erste deutliche Anstieg von im Web geteilten Bildern zu verzeichnen. Ebenso zeitgleich entstanden Soziale Onlinenetzwerke wie Friendster, MySpace und Facebook und ihre Nutzerzahl stieg rasant. Auch sie boten die Möglichkeit, Fotos mit Anderen zu teilen. Die immense Zahl der Nutzer und die Beliebtheit der Dienste – allen voran Facebook – sorgte für eine Explosion der Zahl der geteilten Fotos. Während die Zahl der Fotos bei Flickr von 2004 bis 2010 auf insgesamt 5 Milliarden gestiegen war, vermeldete Facebook eine immense Anzahl monatlich neuer Fotos: 2 Milliarden im September 2009, 3 Milliarden im Februar 2010 [23], 7 Milliarden im Februar 2012 [22] und über 10 Milliarden im September 2013 [61]. Beschleunigt wurde dieses rasante Wachstum der online geteilten Fotos durch die Verbreitung qualitativ hochwertiger Kamera-Handys und Smartphones sowie mobiler Breitband-Datenübertragungstechnik: Diese lösten einen wahren Boom des mobilen Teilens von Fotos aus. So wurden beispielsweise zu Thanksgiving 2012 über mehrere Stunden über 200 Fotos pro Sekunde (entspricht circa 0,5 Mrd. pro Monat) von mobilen Geräten aus beim Onlinedienst Instagram hochgeladen [44]. Während dies in 2012 noch eine Rekordzahl war, verzeichnete der Dienst Ende 2013

täglich 55 Millionen neue Fotos (entspricht circa 1,6 Milliarden pro Monat) [24]. Dieser Boom beschränkte sich nicht nur auf Dienste zum mobilen Teilen von Bildern wie Instagram, PicPlz oder Path, sondern verstärkte auch das Teilen in Sozialen Onlinenetzwerken und anderen Onlinediensten.

Mit dem massiven Teilen von Fotos im Web gelangen so seit einigen Jahren Fotos in eine Teil- oder sogar Weltöffentlichkeit, die zuvor meistens nie das Zuhause von Fotografierenden oder Fotografierten verlassen hätten. Die Fotos gelangen aus dem Kontrollbereich der Nutzer in die (un-)beschränkte Öffentlichkeit und werden somit Ursprung potenzieller Bedrohungen der Privatsphäre – für die teilenden Nutzer selbst und für Andere. Den Menschen fehlt der Überblick über im Web geteilte Bilder, die sie und ihre Privatsphäre in irgendeiner Weise betreffen könnten. Selbst wenn sie einen Teil kennen, können sie sich nicht sicher sein, wie groß der Anteil der bekannten Bilder im Vergleich zu allen potenziell bedrohlichen Fotos ist.

Neben der Online-Verfügbarkeit der Bilder selbst erhöht ein weiterer Faktor die potenzielle Bedrohung durch Bilder: Bild-Metadaten, das heißt Zusatzinformationen zu den Bildern, wie beispielsweise der Ort einer Aufnahme oder auch Namen abgebildeter Personen, können innerhalb von Datenbanken der Onlinedienste oder auch direkt in Bilddateien gespeichert sein. Auch diese können über kurz oder lang dafür sorgen, dass ein Bild zu einer Bedrohung der Privatsphäre wird. Solche Zusatzinformationen können schon seit vielen Jahren von Nutzern manuell in die Bilder eingetragen werden. Aktuell steigt jedoch vor allem die Zahl der von modernen Kameras automatisch hinzugefügten Informationen.

Problem Im Kontext geteilter Fotos fehlt den Nutzern das Bewusstsein über preisgegebene persönliche Informationen sowohl in der Rolle des Fotografen als auch in der Rolle des Fotografierten. Persönliche Informationen können dabei durch ein Fotomotiv und durch zugehörige Metadaten gegeben sein. Diese Informationen werden vom Fotografen oder auch von Anderen, die im Besitz eines Bildes sind, mit dem Bild über das Internet mit Dritten geteilt. Ist eine Person Teil des Fotomotivs, so ist das Motiv selbst eine persönliche Information, die zu einer Bedrohung der Privatsphäre des Abgebildeten führen kann. Außerdem können Zusatzinformationen, wie zum Beispiel der Ort der eigenen Wohnung, die ein Foto zeigt, für den Fotografierten zur Ursache für eine Bedrohung der eigenen Privatsphäre werden. Bild-Metadaten können auch unabhängig vom Motiv Bedrohungen verursachen. Sie können beispielsweise Informationen über den Fotografen enthalten, wie seinen vollständigen Namen oder wann er an welchem Ort gewesen ist.

Während sich diese Arbeit vorwiegend mit geteilten Fotos befasst, existieren vergleichbare Probleme für andere Arten von Social-Media-Inhalten, wie Texte, Videos oder Audioaufnahmen. Einige in Rahmen dieser Dissertation präsentierten Problemlösungen sollten zum Teil auch auf diese übertragen werden können.

1.1.2 Standortbezogene Funktionen mobiler Geräte

Mit der massiven Verbreitung und Nutzung internetfähiger mobiler Geräte wie Smartphones und Tablets wurden diese Geräte eine weitere Quelle für Bedrohungen der Privatsphäre vieler Nutzer. Neben klassischen Basisfunktionen wie Kalender, E-Mail oder Webbrowsen machen vor allem die Vielzahl vielfältiger Anwendungen (kurz: *Apps*), die mobile Internet-Konnektivität und die auf den Geräten verfügbaren Informationen diese zum Schauplatz einer Vielzahl potenzieller Bedrohungen.

Im Fokus stehen dabei die Geräte des Unternehmens Apple sowie Geräte, die das Betriebssystem Android verwenden, da diese einen Großteil des Marktes bilden: Die Marktanteile an der Nutzung von Smartphones betrugen im November 2013 in Deutschland 63,8 % Android und 19,4 % Apple [6] und im Dezember 2013 in den USA 52,2 % Android und 40,6 % Apple [5]. Die Marktanteile am Absatz von Tablets weltweit betrugen im ersten Quartal 2013 48,2 % Apple und 43,4 % Android [42].

Die integrierte Technik der Geräte und die Betriebssysteme ermöglichen die einfache Verwendung persönlicher Kontextinformationen. Folglich werden mit diesen Geräten vermehrt kontextsensitive Dienste genutzt. Auf den mobilen Alleskönnern liegen persönliche Informationen in kondensierter Form vor und der Zugriff auf die Daten ist über standardisierte Schnittstellen möglich. Apps können beispielsweise auf Kontaktinformationen aus dem Adressbuch, E-Mails und andere Nachrichten oder Fotos für die Umsetzung ihrer Funktionen zugreifen.

Insbesondere der aktuelle Aufenthaltsort eines Nutzers ist im mobilen Einsatzbereich eine viel verwendete Kontextinformation. Der Ort wird verwendet, um die aktuelle Position auf einer Karte anzuzeigen, das nächstgelegene Café oder Restaurant zu finden oder Anderen über Apps oder Webdienste zu zeigen, wo man sich gerade aufhält. Laut einer Studie des Pew Internet & American Life Projects aus dem Mai 2012 [37] nutzten 74 % der amerikanischen Smartphone-Besitzer standortbezogene Dienste, um aktuelle Informationen zu erhalten, und 18 % der Smartphone-Besitzer nutzten Webdienste, um ihren aktuellen Aufenthaltsort mit Anderen zu teilen.

Neben dem klassischen Diebstahl von persönlichen Informationen wie dem gespeicherten Adressbuch oder dem aktuellen Aufenthaltsort eines Nutzers stellt auf den mobilen Geräten vor allem auch die aktive Preisgabe dieser Informationen durch den Nutzer selbst die Basis für potenzielle Bedrohungen dar. Nutzt ein Nutzer eine App, die beispielsweise Anderen mitteilt, wo er sich hin und wieder befindet, so gibt er der App die Rechte zum Zugriff auf seinen Standort und erlaubt ihr bewusst und freiwillig die Nutzung dieser Information. Aufgrund geringer Transparenz weiß er jedoch beispielsweise nicht, wann genau die App auf diese Information zugreift und seinen aktuellen Aufenthaltsort verwendet. Spielt der Nutzer ein Spiel, das identische Zugriffsrechte auf persönliche Informationen bei der Installation verlangt, welches jedoch keine ersichtliche Funktion mit Ortsbezug bietet, tappt der

Nutzer in Bezug auf die Verwendung seiner Informationen völlig im Dunklen. Die aktuellen Systeme geben ihm keine Möglichkeit die preisgegebenen Informationen zu beschränken. Vielmehr bleibt dem Nutzer nur die Entscheidung eine Funktion/App zu nutzen oder auf die Nutzung zu verzichten.

Problem Apps auf mobilen Geräten bieten heute eine Vielzahl hilfreicher Funktionen, die den persönlichen Kontext der Nutzer berücksichtigen. Um diese zu nutzen, gewähren die Nutzer vielen Apps und damit den App-Erstellern beziehungsweise Dienstanbietern Zugriff auf ausgewählte persönliche Informationen, die die Grundlage von Bedrohungen ihrer Privatsphäre werden können. Besonders der aktuelle Standort der Nutzer wird häufig von Apps verwendet. Er kann zur Überwachung der Nutzer missbraucht werden oder zu anderem Schaden für ihre Privatsphäre führen. Wurde der Zugriff auf den aktuellen Ort erlaubt, kann eine App diesen, wann und wie oft sie möchte, verwenden. Es fehlt an Bewusstsein über die Verwendung der einmal bewusst freigegebenen Daten. Funktionen zur Schaffung von Transparenz und detaillierte Kontrollmöglichkeiten fehlen auf den heutigen Geräten.

1.2 Ziel der Dissertation

Sowohl durch das Teilen von Fotos im Web als auch durch die Nutzung von Standortinformationen auf mobilen Geräten werden persönliche Informationen von Nutzern gegenüber anderen Personen, Institutionen, Firmen oder der Öffentlichkeit preisgegeben. Diese Informationen können zu Bedrohungen der Privatsphäre und zu Schaden für die betroffenen Personen führen. Ein grundlegendes Problem ist dabei, dass den Nutzern nicht immer bewusst ist, wann und wo sie oder Andere mit ihren persönlichen Informationen agieren oder diese preisgeben. Folglich kann ihnen auch nicht immer bewusst sein, dass ihre Privatsphäre bedroht sein könnte. Ein Teil der Nutzer ist sich der Problematik generell nicht bewusst. Andere, die meinen sich über die möglichen Bedrohungen generell im Klaren zu sein, fühlen sich eventuell nicht betroffen, auch wenn sie betroffen sind, und wägen sich in falscher Sicherheit. Um beidem zu begegnen, wird im Rahmen dieser Dissertation die Problematik des fehlenden Bewusstseins betrachtet.

Ziel dieser Dissertation ist, die grundlegende Problematik aufzuzeigen und am Beispiel der zwei zuvor genannten Anwendungsfälle zu untersuchen. Für die beiden Anwendungsfälle werden im Rahmen der Untersuchung entwickelte Methoden präsentiert, die dazu dienen, das Bewusstsein und die Kontrolle der Nutzer über die Verwendung und die Verbreitung persönlicher Informationen zu stärken, um ihnen zu ermöglichen ihre Privatsphäre besser zu schützen. Die Nutzer müssen auf lange Sicht befähigt werden, zu wissen, wann und wo sie oder Andere persönliche oder personenbezogene Informationen preisgeben. Sie sollen befähigt werden, etwas ge-

gen durch sich selbst oder durch Andere verursachte Bedrohungen zu tun und wo möglich die Preisgabe von Informationen einzuschränken. Unter der Prämisse, dass viele Angebote im Social Web und Funktionen kontextsensitiver Dienste auf der Preisgabe persönlicher Informationen beruhen, sollen die Nutzer befähigt werden, ihre persönlichen Informationen bewusst, fundiert und dosiert preiszugeben. Dies soll ihnen ermöglichen, den Mehrwert gebotener Funktionen zu nutzen und gleichzeitig ihre Privatsphäre so weit es möglich und gewünscht ist zu schützen.

1.3 Wissenschaftlicher Beitrag

Diese Dissertation untersucht das Bewusstsein der Nutzer über die Preisgabe von persönlichen Informationen durch im Web geteilte Bilder und durch die Nutzung standortbezogener Funktionen auf mobilen Geräten. Es wird gezeigt, dass eine klare Diskrepanz zwischen dem existierenden Bewusstsein und dem für die Wahrung der Privatsphäre notwendigen Bewusstsein besteht. Um diese Diskrepanz zu minimieren, werden Methoden zur Schaffung und Verbesserung des Bewusstseins präsentiert, die den Nutzern helfen können, ihre eigene Privatsphäre zu schützen und die Privatsphäre Anderer nicht unnötig zu gefährden. Außerdem werden Methoden präsentiert, die die Kontrolle über persönliche Informationen und die Transparenz ihrer Verwendung verbessern. Insbesondere werden dazu folgende Einzelbeiträge geleistet:

- Durch die Evaluierung verschiedener Webdienste zum Teilen von Fotos wird gezeigt, wie die heutigen Webdienste geteilte Bilder und deren Metadaten handhaben und vor unerwünschtem Zugriff schützen. Es wird ein deutlicher Verbesserungsbedarf identifiziert. Durch die Analyse von Bild-Datensätzen der Dienste Flickr und Locr wird gezeigt, wie ausgeprägt die Nutzung von Metadaten heute ist. Die Erhebung zeigt, dass die Menge der Metadaten geteilter Bilder so groß ist, dass diese als ernstzunehmende Bedrohung gesehen werden müssen. Durch beide Erhebungen wird untermauert, dass eine realistische Bedrohung nicht nur durch Bilder, sondern auch durch deren Metadaten besteht.

- Auf Basis zweier Nutzerstudien zum Teilen von Fotos im Web wird – allgemein sowie speziell am Beispiel des Sozialen Onlinenetzwerkes Facebook – gezeigt, wie (un-)bewusst sich die Nutzer über die Preisgabe persönlicher Informationen durch Bilder und Metadaten sind, welche Andere im Web teilen. Es wird gezeigt, dass das Bewusstsein der Nutzer nicht ausreichend ist und in Zahlen festgehalten, wie falsch sie das Ausmaß der potenziellen Bedrohung ihrer Privatsphäre einschätzen. Die Ergebnisse geben Aufschluss über die heutigen Nutzer und motivieren weitere Arbeiten, die zum Ziel haben, Bewusstsein zu schaffen und die Nutzer durch technische Lösungen zu unterstützen.

- Das Konzept von *Privatheitsstufen* persönlicher Informationen und eines darauf aufbauenden *Privatsphäre-Kompromisses* als Grundlage für den Schutz der Privatsphäre wird vorgestellt. Durch Studienergebnisse wird gezeigt, dass das präsentierte Konzept für einen nennenswerten Teil der Nutzer ein probates Mittel wäre, ihre Privatsphäre besser zu schützen. Die Bereitschaft weniger private Informationen gegen den Schutz mehr privater Informationen einzutauschen zeigt ein Verständnis von Privatheit von Informationen, das über die klassische Einordnung in privat oder öffentlich hinausgeht.

- Es werden verschiedene technische Ansätze vorgestellt, die Nutzer unterstützen können, von geteilten Fotos im Web zu erfahren, welche ihre Privatsphäre betreffen könnten. Es werden Konzepte für einen Dienst zur Unterstützung der proaktiven Suche nach bedrohlichen Bildern präsentiert. Außerdem wird ein Dienst vorgestellt, der basierend auf Privatsphäre-Kompromissen Nutzer aktiv über sie potenziell betreffende Fotos informieren kann, sobald diese geteilt wurden. Die Umsetzbarkeit der Dienste wird diskutiert, durch Simulation grundlegend evaluiert und teilweise durch Implementierung gezeigt.

- In Form einer Erweiterung für den Webbrowser Chrome wird ein Ansatz vorgestellt, wie Nutzern ermöglicht werden kann, integrierte Metadaten im Web geteilter Bilder mit dem Fokus auf private Informationen zu visualisieren und die Preisgabe integrierter Metadaten beim Hochladen der Bilder zu kontrollieren. Durch Ergebnisse einer Laborstudie wird gezeigt, wie positiv die Nutzbarkeit und die gebotenen Funktionen der Erweiterung von Nutzern empfunden wurden. Des Weiteren wird durch diese gezeigt, dass die Nutzer willens wären, Verschlüsselung zum Schutz und Erhalt von Metadaten zu verwenden.

- Es wird ein Framework zur einfachen Implementierung von Methoden zur Verschleierung von Standortinformationen für das mobile Betriebssystem Android vorgestellt. Die Erweiterung des Betriebssystems ermöglicht es Verschleierungsmethoden in der Praxis zu evaluieren, welche bisher oft nur theoretisch beschrieben oder durch Simulation erprobt worden sind. Technisch versierten Nutzern erlaubt die Implementierung, eine für jede App individuelle Methode zum Schutz ihres aktuellen Aufenthaltsortes zu bestimmen.

- Eine auf den Ergebnissen von Fokusgruppen-Diskussionen aufbauende Erweiterung des Betriebssystems Android wird präsentiert. Sie zeigt, wie eine einfach zu bedienende Umsetzung von Standortverschleierung Nutzern ermöglichen kann, für jede App den individuellen Grad an Privatheit zu bestimmen, den sie für angemessen halten. Dies zeigt, wie die Nutzung standortbezogener Dienste und der Schutz der Privatsphäre vereint werden können. Es wird zu-

dem gezeigt, wie unentschiedene Nutzer bei den wenigen Entscheidungen, die zur Konfiguration notwendig sind, durch einen crowdsourcing-basierten Dienst unterstützt werden können, indem ihnen gezeigt wird, welche Einstellungen Andere wählten.

- Eine für die Untersuchung von IT-Sicherheit und Privatsphäre auf mobilen Geräten entwickelte Simulationslösung wird präsentiert, die im Rahmen von Vorarbeiten zu dieser Dissertation entstanden ist und im Rahmen dieser Dissertation zur Evaluierung eines vorgestellten Dienstes verwendet wird.

Ein Teil der präsentierten wissenschaftlichen Beiträge wurde im Rahmen der Entstehung dieser Dissertation in folgenden internationalen Publikationen veröffentlicht:

1. B. Henne, C. Szongott, M. Smith: *SnapMe If You Can: Privacy Threats of Other Peoples' Geo-tagged Media and What We Can Do about It*, 6$^{\text{th}}$ ACM Conference on Security and Privacy in Wireless and Mobile Networks, 2013.
2. M. Smith, B. Henne, C. Szongott, G. von Voigt: *Big Data Privacy Issues in Public Social Media*, 6$^{\text{th}}$ IEEE International Conference on Digital Ecosystems Technologies, 2012.
3. B. Henne, M. Smith: *Awareness about Photos on the Web and How Privacy-Privacy-Tradeoffs Could Help*, Financial Cryptography and Data Security, Workshop on Usable Security, LNCS 7862, Springer, 2013.
4. B. Henne, M. Harbach, M. Smith: *Location Privacy Revisited: Factors of Privacy Decisions*, Extended Abstracts on Human Factors in Computing Systems, ACM, 2013.
5. B. Henne, M. Linke, M. Smith: *A study on the Unawareness of Shared Photos in Social Network Services*, IEEE Security and Privacy Workshop on Web 2.0 Security and Privacy, 2014.
6. B. Henne, M. Koch, M. Smith: *On the Awareness, Control and Privacy of Shared Photo Metadata*, Financial Cryptography and Data Security, LNCS 8437, Springer, 2014.
7. B. Henne, C. Kater, M. Smith: *Selective Cloaking: Need-to-know for Location-based Apps*, 11$^{\text{th}}$ International Conference on Privacy, Security and Trust, IEEE, 2013.
8. B. Henne, C. Kater, M. Smith: *On Usable Location Privacy for Android with Crowd-Recommendations*, 7$^{\text{th}}$ International Conference on Trust and Trustworthy Computing, LNCS 8564, Springer, 2014.

Die im Rahmen von Vorarbeiten entwickelte Simulationslösung zur Evaluierung mobiler Szenarien wurde zudem in folgenden Arbeiten wissenschaftlich publiziert:

9. B. Henne, C. Szongott, M. Smith: *Towards a Mobile Security & Privacy Simulator*, IEEE Conference on Open Systems, 2011.
10. B. Henne, C. Szongott, M. Smith: *Coupled Multi-agent Simulations for Mobile Security & Privacy Research*, 6$^{\text{th}}$ IEEE International Conference on Digital Ecosystems Technologies, 2012.

1.4 Aufbau der Dissertation

Dieses Kapitel führte in das Thema der vorliegenden Dissertation ein, stellte das identifizierte Problem vor und erläuterte die Ziele der Dissertation.

Um den Lesern ein besseres Verständnis der präsentierten Arbeiten und Resultate zu ermöglichen, werden in Kapitel 2 Begriffe erläutert und Grundlagen vertieft.

Für eine Einordnung dieser Dissertation in das wissenschaftliche Umfeld werden in Kapitel 3 ausgewählte andere wissenschaftliche Arbeiten und Entwicklungen vorgestellt, die bis dato im Themenfeld dieser Dissertation entstanden sind.

In Kapitel 4 werden für die beiden gewählten Anwendungsfälle, geteilte Fotos im Social Web und standortbezogene Funktionen mobiler Geräte, Ursachen und Faktoren für Bedrohungen der Privatsphäre analysiert, die durch das zuvor identifizierte Problem und die in den Anwendungsfällen vorhandenen Informationen entstehen.

Kapitel 5 befasst sich mit dem Bewusstsein der Nutzer über im Social Web geteilte Fotos. Es gibt einen Überblick über Schutzmaßnahmen und den Umgang mit Bild-Metadaten verschiedener Webdienste. Exemplarisch wird am Beispiel der Dienste Flickr und Locr gezeigt, in welchem Ausmaß heute Metadaten zusammen mit Bildern geteilt werden. Es werden zwei Studien vorgestellt, die sich mit dem Bewusstsein der Nutzer befassen. Die erste Studie erfasste das Bewusstsein über geteilte Fotos und Metadaten im Allgemeinen. Sie evaluiert außerdem das Konzept von Privatsphäre-Kompromissen als Basis für Schutzmaßnahmen. Die zweite Studie erfasste am Beispiel des Sozialen Onlinenetzwerkes Facebook, inwieweit sich die Nutzer über das Ausmaß geteilter Bilder bewusst sind, die ihre Privatsphäre betreffen könnten. Aufbauend auf den Erhebungen und Studienergebnissen werden Konzepte zur Unterstützung der proaktiven Suche nach relevanten Fotos vorgestellt. Außerdem wird ein Dienst präsentiert, der Nutzer basierend auf Privatsphäre-Kompromissen aktiv über relevante Fotos benachrichtigt, sobald diese hochgeladen wurden. Die Umsetzbarkeit des Dienstes wird durch Simulation und durch eine Proof-of-Concept-Implementierung grundlegend evaluiert.

Kapitel 6 befasst sich speziell mit eingebetteten Bild-Metadaten. Es wird eine Browser-Erweiterung vorgestellt, die der Schaffung von Bewusstsein über Metadaten von Bildern im Moment ihres Teilens dient, sowie dem Bewusstsein über Metadaten bereits geteilter Bilder. Die Erweiterung implementiert prototypisch einen Ansatz, der ermöglicht, Metadaten im Moment des Teilens zu verändern. Es wird ein Konzept vorgestellt, wie auf Basis von Verschlüsselung Metadaten geteilt werden können, ohne sie der breiten Masse preisgeben zu müssen. Die Ergebnisse einer Laborstudie zeigen eine ausgeprägte positive Akzeptanz der Nutzer gegenüber der Erweiterung.

Kapitel 7 befasst sich mit der Schaffung von Bewusstsein über die Verwendung von Standortinformationen im Kontext mobiler Geräte und dem Schutz der Privatsphäre durch die Verschleierung der Ortsinformationen. Es wird ein Framework vorgestellt, das der Evaluierung von Methoden zur Standortverschleierung auf mobilen Geräten dient. Eine auf dieser Erweiterung des Android-Betriebssystems und den Ergebnissen von Fokusgruppen-Diskussionen basierende nutzerfreundliche Umsetzung von Standortverschleierung wird vorgestellt, die die Nutzung standortbezogener Dienste ermöglicht, während die Privatsphäre der Nutzer maximal geschützt bleibt. In Form eines crowdsourcing-basierten Dienstes werden die Nutzer bei der Konfiguration unterstützt.

In Kapitel 8 werden abschließend die in dieser Dissertation präsentierten Arbeiten zusammengefasst. In Kapitel 9 wird ein Ausblick auf mögliche anschließende Forschungsarbeiten gegeben.

Anhang

Der Anhang enthält ergänzende Detailinformationen.

Anhang A umreißt die Simulationslösung, auf der die in Kapitel 5 beschriebene Evaluierung aufbaut. Die Software und die dazugehörigen wissenschaftlichen Arbeiten waren in Vorarbeiten zu dieser Dissertation entstanden.

In Anhang B werden weitere Details zu den in Kapitel 5 erhobenen Daten zur Verwendung und Verbreitung von Bild-Metadaten gegeben.

In Anhang C werden Materialien, Detailinformationen zu den durchgeführten Studien und Fragebögen inklusive Teilnehmerantworten zur Verfügung gestellt, so dass die Studien besser von den Lesern nachvollzogen werden können.

Kapitel 2

Grundlagen

In diesem Kapitel werden Begriffe erläutert und technische Grundlagen vertieft, um ein besseres Verständnis der präsentierten Arbeiten und Resultate zu ermöglichen.

2.1 Begriffsdefinitionen: vom Internet zum Social Web

Begriffe wie das Internet, das Web, oder soziale Medien werden häufig unscharf und teilweise sogar synonym verwendet. Um Unklarheiten zu vermeiden, werden die in dieser Dissertation verwendeten Begriffe im Folgenden definiert.

Das ***Internet*** ist ein weltweites Netzwerk von Rechnernetzwerken, das Computer und andere technische Geräte auf der ganzen Welt miteinander verbindet und so den Datenaustausch zwischen diesen ermöglicht. Es ging ursprünglich aus dem Arpanet hervor, einem Projekt der Advanced Research Project Agency (ARPA) des US-Verteidigungsministeriums aus dem Jahre 1969. Das Internet bildet die Grundlage für diverse Internetdienste, wie E-Mail, das Abrufen von Webseiten oder den Datenaustausch zwischen entfernten Rechnern.

Das ***World Wide Web*** (WWW, kurz: *Web*) ist ein Internetdienst für den Abruf von elektronischen Hypertext-Dokumenten, kurz Webseiten. Das zugrunde liegende Internet-Protokoll HTTP wurde zu Beginn der 1990er-Jahre bei der Europäischen Organisation für Kernforschung (CERN) entwickelt. Mit der Schaffung von grafischen Webbrowsern wurde das Web nach kurzer Zeit auch für Laien zugänglich gemacht. Während es anfänglich dem Austausch statischer Inhalte diente, sind mit der Zeit immer mehr dynamische Inhalte entstanden. Heute dient es oft auch als Nutzerschnittstelle zu anderen Internetdiensten, wie beispielsweise E-Mail.

Der Begriff ***Web 2.0*** beschreibt eine Weiterentwicklung des klassischen World Wide Webs. Das Web wurde nach der Jahrtausendwende zu einer Plattform für Onlinedienste, die Nutzern erlauben, miteinander zu agieren und zu kollaborieren. Während im klassischen Web die Inhalte von Informationsanbietern wie Firmen

erstellt wurden und die Nutzer diese lediglich konsumierten, ermöglichen Web-2.0-Dienste den Nutzern Inhalte auch zu produzieren. Die Nutzer werden zu sogenannten Prosumenten – Produzenten und Konsumenten in einer Person. Beispiele für Web-2.0-Angebote sind Wikis, Online-Tagebücher in Form von Weblogs (Blogs) oder Online-Communitys wie YouTube oder Flickr.

Der Begriff ***Social Media*** (im Deutschen: *Soziale Medien*) beschreibt Dienste im Web, die es Nutzern ermöglichen sich auszutauschen und mediale Inhalte gemeinsam zu erstellen oder sie miteinander zu teilen. Social-Media-Dienste basieren auf den Techniken des Web 2.0. Sie heben sich jedoch durch den Fokus auf die Interaktion der Nutzer von diesem ab. Die Vernetzung in Form von sozialen Netzwerken spielt eine große Rolle. Nutzer können Inhalte erstellen, Inhalte anderer weiterempfehlen oder weiterverbreiten und ihre Meinungen miteinander austauschen. Besonders die Weiterverbreitung von Inhalten beruht dabei stark auf den Strukturen der sozialen Netzwerke der Nutzer, ihrem „Online-Freundeskreis“. Beispiele für Social Media sind Soziale Onlinenetzwerke wie Facebook oder Mikroblogging-Dienste wie Twitter. Durch die Integration von sozialen Netzwerken und Funktionen für die Interaktion zwischen Nutzern entwickeln sich viele Web-2.0-Angebote zu Social Media.

Der Begriff der ***sozialen Netzwerke*** entstammt ursprünglich der Soziologie und beschreibt gegebene soziale Interaktionsstrukturen von Menschen, wie etwa Bekanntschaftsnetzwerke. Dienste im Web, die solche Interaktionsstrukturen abbilden und in Funktionen integrieren, werden im Deutschen ebenfalls häufig als soziale Netzwerke bezeichnet. Zur Differenzierung werden solche Onlinedienste im Rahmen dieser Dissertation ausschließlich als Soziale Onlinenetzwerke bezeichnet.

Soziale Onlinenetzwerke sind Dienste im Web, die Nutzern den Aufbau und die Pflege von sozialen Kontakten ermöglichen. Im Vergleich zu Online-Communitys sind Soziale Onlinenetzwerke auf die einzelnen Nutzer fokussiert anstatt auf einen gemeinsamen Austausch zu einem bestimmten Zweck oder Thema. Ein Nutzer präsentiert sich selbst meist durch ein persönliches Profil. Durch den Aufbau einer Kontaktliste (häufig: *Freundesliste*) pflegt der Nutzer sein soziales Netzwerk innerhalb des Dienstes. Häufige Funktionen sind das Schreiben und Lesen von persönlichen Nachrichten, das öffentliche oder beschränkt-öffentliche Teilen eigener Kurznachrichten oder Medieninhalte wie Fotos, Videos oder Tonaufnahmen, das Weiterverbreiten und Kommentieren von Inhalten anderer oder die Benachrichtigung über Ereignisse und Inhalte im eigenen sozialen Netzwerk. Soziale Onlinenetzwerke sind das Paradebeispiel für Social Media. Sie existieren in allgemeinen Ausprägungen, wie beispielsweise Facebook, Google+, meinVZ/studiVZ oder MySpace, sowie auch mit einem Themenfokus, wie die Karrierenetzwerke Xing oder LinkedIn.

Das ***Social Web*** umfasst alle auf Web-2.0-Techniken aufbauenden Vorkommen von sozialen Strukturen und Interaktionen zwischen Nutzern im World Wide Web.

Als Oberbegriff beinhaltet es somit Social Media sowie Soziale Onlinenetzwerke. Einen weiteren Aspekt des Social Webs bilden kollaborative Ansätze wie das Crowdsourcing oder das Crowdfunding.

Crowdsourcing bezeichnet die Auslagerung bestimmter Aufgaben an eine Gruppe freiwilliger Personen. Der Begriff ist angelehnt an den Begriff des Outsourcings, der die Auslagerung von Unternehmensaufgaben an Drittunternehmen beschreibt. Heute findet der Begriff seine hauptsächliche Verwendung im Kontext des Web 2.0, auf dessen Basis Aufgaben an ein Kollektiv von Personen des Social Webs ausgelagert werden. Eine spezielle Form stellt das mobile Crowdsourcing dar, bei dem Aufgaben an Besitzer mobiler Geräte ausgelagert werden und für die Erfüllung der Aufgaben auf Funktionen der Geräte zurückgegriffen werden kann, wie die Bestimmung des aktuellen Ortes, das Erstellen von Fotos und den mobilen Internetzugang. Crowdsourcing-Projekte erstrecken sich von wissenschaftlichen Untersuchungen wie der Lärmpegelmessung in Städten, über die Informationssammlung beim Katastrophenschutz oder Auftragsfotografie bis hin zur Ideenfindung in Kreativprozessen.

2.2 Metadaten

Metadaten sind Daten, die andere Daten beschreiben. Die amerikanische *National Information Standards Organization* (NISO) definiert sie als „strukturierte Informationen, die eine Informationsressource beschreiben, erklären, verorten oder auf eine andere Weise das Beziehen, Nutzen oder Verwalten dieser erleichtern“ [68]. Metadaten beziehungsweise *Metainformationen* werden oft auch als Daten über Daten oder Informationen über Informationen bezeichnet.

Das Konzept der Metadaten ist schon seit Jahrhunderten in Bibliotheken in Verwendung, in denen Bücherkataloge den Überblick und den Zugriff auf große Buchbestände erleichtern. Mit der immer stärker steigenden Zahl an digitalen Inhalten wird dieses Konzept immer mehr in die digitale Welt übernommen. So sind Metadaten heute in verschiedensten Bereichen zu finden: in Online-Katalogen von Bibliotheken, als Autorenangaben von Webseiten, als eingebettete Inhaltsbeschreibungen digitaler Medien oder in Form von Ortsangaben zu Mikroblog-Beiträgen.

Allgemein unterscheidet man administrative, strukturelle, technische und deskriptive Metadaten. Administrative Metadaten beschreiben beispielsweise die Herkunft, Speicherung und die Zugriffsrechte auf ein Dokument. Strukturelle Metadaten beschreiben die Struktur von Daten, beispielsweise die Einteilung eines Dokumentes in Kapitel. Die Beschreibung der digitalen Speicherung wie etwa Kodierverfahren werden unter dem Begriff der technischen Metadaten zusammengefasst. Diese drei Arten von Metadaten dienen vor allem der Datenbeherrschung an sich und haben besondere Bedeutung für Institutionen oder Unternehmen wie Softwarehersteller,

die sich mit dem Thema der Speicherung von Daten auseinandersetzen.

Deskriptive Metadaten sind im Gegensatz dazu besonders für die Nutzer von Bedeutung. Ihr Zweck ist, Angaben zu Inhalten von Dokumenten zu machen, wie etwa ihre Verfasser, Titel oder Schlagworte zur Klassifizierung der Inhalte. Für einen Nutzer, der primär an den Inhalten interessiert ist, können solche Metadaten den Überblick, die Ordnung und Suche erleichtert, besonders wenn die Zahl der zu überblickenden Inhalte stetig wächst. Neben Textdokumenten gilt dies insbesondere für digitale Medien wie Filme und Bilder, die mit den heutigen technischen Mitteln aufgrund der Komplexität der Daten nicht ohne Weiteres zu durchsuchen sind. Beispielsweise können aus Tausenden von Bildern oder Filmen diejenigen, die den Eiffelturm in Paris zeigen, weitaus effizienter gefunden werden, wenn die entsprechenden Bilder das Schlagwort „Eiffelturm“ oder auch nur „Paris“ enthalten, als wenn alle Bilder mit einem entsprechenden Vergleichsbild abgeglichen werden müssen. Zudem können Metadaten über den Ort der Aufnahmen dafür sorgen, dass Kopien des Pariser Wahrzeichens in aller Welt nicht im Suchergebnis enthalten sind.

2.2.1 Standardisierung

Für die einheitliche Verwendung und Vergleichbarkeit von Metadaten verschiedener Informationsressourcen ist eine Standardisierung der Beschreibung von Metainformationen notwendig. Schon in klassischen Bibliotheken wurde daher beispielsweise die international verbreitete Dewey-Dezimalklassifikation oder die Dezimalklassifikation nach Gottfried Wilhelm Leibniz eingeführt. Im Bereich digitaler Medien gibt es heute eine Vielzahl domänenspezifischer (de-facto) Standards, die weit über solche einfachen Ordnungssysteme hinausgehen. Sie werden meist von Firmen oder übergreifenden Gremien formuliert und gepflegt. Bekannte Vertreter von Metadaten-Standards sind beispielsweise:

- *Digital Object Identifier* (DOI) definiert eindeutige und dauerhafte digitale Identifikatoren für physische, digitale oder abstrakte Objekte. Sie sind vergleichbar mit der Internationalen Standardbuchnummer (ISBN).

- *Dublin Core* (DC) ist eine Sammlung von Metainformationen zur Beschreibung von Objekten im Internet. Es umfasst unter anderen den Titel, das Thema, die Autoren oder die Rechteinhaber eines Objektes.

- *Resource Description Framework* (RDF) ist ein allgemeines Datenmodell für Metadaten aus dem Bereich des Semantic Webs. Es basiert auf der *Extensible Markup Language* (XML). RDF kann für die Beschreibung verschiedenster Ressourcen verwendet werden.

2.2.2 Speicherung

Metadaten digitaler Inhalte werden auf verschiedene Weisen gespeichert. Der Ort der Speicherung hat dabei einen direkten Einfluss auf die Weitergabe der Metadaten mit einer beschriebenen Informationsressource.

1. Metadaten werden innerhalb einer beschriebenen Informationsressource gespeichert. In diesem Fall ist die Verknüpfung von Daten und Metadaten von sich aus gegeben. Die Metadaten verbleiben immer dort, wo auch die Daten sind. Werden die Daten kopiert und weitergegeben, so auch die Metadaten.

2. Metadaten werden neben einer Informationsressource im selben Kontext gespeichert. Im Fall von Dateien werden sie häufig in einer separaten *Sidecar*-Datei im selben Verzeichnis gespeichert. Daten und Metadaten sind nur lose gekoppelt. Werden die Daten kopiert, so werden die Metadaten nicht mit diesen kopiert. Sie können jedoch auch dieselbe Weise weitergegeben werden.

3. Metadaten werden separat gespeichert und nur durch eine Referenz auf eine Informationsressource mit dieser verknüpft. Beispiele hierfür sind die Speicherung von Metadaten zu Dateien in der Datenbank einer Dateiverwaltungssoftware und die Speicherung von Metainformationen in Datenbanken von Webdiensten. Der Bezug zwischen Metadaten und Daten wird durch eindeutige Bezeichner wie URIs hergestellt. Die Informationen sind nur lose gekoppelt. Die Weitergabe der Metadaten ist schwieriger, da sie in anderer Form als die Daten selbst gespeichert sind.

Neben dem Ort kann sich auch das Speicherformat der Metadaten unterscheiden, welches häufig durch Standards bestimmt wird. Gängige Speicherformate reichen von proprietären Binärdaten bis zu textuellen Schlüssel-Wert-Paaren oder XML.

2.2.3 Eingebettete Metadaten digitaler Bilder

Ein großer Teil der digitalen Bilder enthält heute eingebettete Metadaten. Dies ist zum einen damit zu begründen, dass heutige Kameras und Software Metadaten teilweise automatisch oder semi-automatisch in Bildern speichern, während diese früher rein manuell durch die Nutzer ergänzt wurden. Zum anderen scheint der Wert von Metadaten im Fall von Bildern höher zu sein, als es beispielsweise bei Office-Dokumenten der Fall ist: Während für viele Nutzer der Titel und die Bedeutung eines Office-Dokumentes eventuell direkt im Dateinamen stecken, bieten die Metadaten von Bildern ein für viele interessanteres und auch größeres Spektrum an Zusatzinformationen, die ein Bild oder Video mit Kontextinformationen anreichern können: Titel, Thema, Inhalt, Fotograf, Ort einer Aufnahme oder auch Urheberrechtsinhaber können so neben dem Bild selbst gespeichert werden. Ein weiterer

Grund ist wohl, dass die Presse und Bildagenturen den Vorteil von Metadaten für Medien schon zu Beginn des digitalen Zeitalters erkannt haben und so als treibende Kraft für die Schaffung von Standards und deren Verbreitung gesorgt haben.

Durch die Etablierung verschiedener Standards wurde über die Jahre zulasten von Softwareanbietern und Nutzern auch Komplexität geschaffen. Drei verschiedene Metadaten-Standards sind heute gleichzeitig aktuell: *Exif*, *IPTC* und *XMP*. Die Standards ergänzen sich nur teilweise. Vielmehr existiert eine nennenswerte Überdeckung der abgebildeten Kontextinformationen bei den Standards, die aufgrund von (Abwärts-)Kompatibilitätsanforderungen alle umgesetzt werden sollten. Das Gros der verfügbaren Software unterstützt jedoch nur einen Teil der Standards oder auch nur einen Teil der abgebildeten Informationen.

2.2.3.1 Exif-Metadaten

Das *Exchangeable Image File Format* (Exif) definiert einen Standard zur Speicherung von Metadaten in Bilddateien. Der Standard wurde im Oktober 1995 von der *Japan Electronic Industry Development Association* etabliert und wurde letztmals im Mai 2013 aktualisiert. Die neuste Auflage Exif Version 2.3 [65] wurde gemeinsam von der *Japan Electronic and Information Technology Industries Association* und der *Camera & Imaging Products Association* formuliert.

Exif-Metadaten werden im Header-Bereich der jeweiligen Bilddatei gespeichert. Unterstützt werden Bilder in den Formaten JFIF/JPEG und TIFF. Exif ist momentan das verbreitetste Format zur Speicherung von Bild-Metadaten. Es ist ein Binärformat: Struktur, Datentypen, Feldlängen und Kodierung der Metadaten werden durch den Standard festgelegt. Exif-Metadaten dienen vorwiegend der Speicherung technischer Informationen zu Aufnahmen durch Kameras.

Alle heute gängigen Digitalkameras, sowie Kamera-Handys und Smartphones schreiben Metadaten in diesem Format in geschossene Fotos. Exif-Metadaten speichern neben dem Kamerahersteller und Kameramodell beispielsweise Informationen zur Bildorientierung oder die Objektiv- und Blitzeinstellungen. Der Exif-Standard ermöglicht und empfiehlt das Speichern eines Vorschaubildes im Rahmen der Bild-Metadaten. Dies ermöglicht das schnellere indexieren großer Bildbestände. Moderne Kameras, Tablets und Smartphones speichern zudem den Ort eines Bildes in Form von geographischen Koordinaten in den Exif-Metadaten. In Form der sogenannten *Maker Notes* können Hersteller proprietäre Daten speichern, so dass die Vielfalt der Metainformationen zum Teil auch herstellerabhängig ist. In den Maker Notes speichern beispielsweise aktuelle Kameras der Marke Canon eine eindeutige Seriennummer der Kamera sowie einen vom Nutzer festgelegten Namen des Kamerabesitzers. Auch Software zur Bildbearbeitung unterstützt am häufigsten Exif-Metadaten.

2.2.3.2 XMP-Metadaten

Die *Extensible Metadata Platform* (XMP) ist ein Standard um Metadaten in digitale Medien einzubetten. Der XMP-Standard wurde im Jahr 2001 von der Firma *Adobe Systems* veröffentlicht. Der Kernteil der Spezifikation [56] wurde im Jahr 2012 zum ISO-Standard *ISO 16684-1:2012*. XMP basiert auf den offenen Standards der *Extensible Markup Language* (XML) und des *Resource Description Frameworks* (RDF). Die in XML/RDF beschriebenen Metadaten können in die Binärdaten verschiedener Mediendateien wie JPEG-, TIFF-, PNG-, DNG-Bilder oder PDF-Dateien eingebettet werden oder in Form von Sidecar-Dateien gespeichert werden [58].

Der zweite Teil der XMP-Spezifikation [57] definiert grundlegende Metainformationen, die gespeichert werden können. Die Informationen werden dabei durch XML Namespaces strukturiert. Beispiele hierfür sind die Namespaces für *PDF*-Dateien, *Photoshop*-Informationen oder Metadaten gemäß Dublin Core. Auch die Metainformationen des Exif-Standards werden durch einen eigenen Namespace in XMP abgebildet [60]. Die Menge der abgebildeten Metainformationen des XMP-Standards wird durch verschiedene XML-Schema-Definitionen von Softwareherstellern wie *Microsoft* oder Gremien wie der *Metadata Working Group* (MWG) erweitert.

2.2.3.3 IPTC-Metadaten

Das *Information Interchange Model* (IIM) [62] wurde für einen verbesserten Austausch von Informationen zwischen Nachrichtenagenturen und Zeitungen vom *International Press Telecommunications Council* (IPTC) zusammen mit der *Newspaper Association of America* (NAA) entwickelt und im Jahre 1991 veröffentlicht. Das IIM definiert die Metainformationen, die zu einem Objekt gespeichert werden können, sowie ein binäres Format, das die einzelnen Einträge in einer Struktur kombiniert. Die Einträge unterliegen zum Teil festen Längen- und Formatbeschränkungen. Für die Weitergabe von Fotos zusammen mit ihren Metadaten wird gemäß des IIM das jeweilige Datenobjekt mit seinen Metadaten in eine im Standard definierte Datenstruktur verkapselt. Mit der Entwicklung moderner Datenrepräsentationen wie XML wurde die Weiterentwicklung des IIM mit Version 4.1 im Jahre 1997 eingestellt.

Mitte der 1990er-Jahre integrierte der Softwarehersteller *Adobe Systems* das Speichern und Lesen von Metadaten in seine Software *Photoshop*. Dabei orientierte sich der Softwarehersteller an den im IIM definierten Metainformationen, speicherte diese jedoch innerhalb der Header der jeweiligen Bilddateien. Im Laufe der Zeit adaptierten auch andere Bildbearbeitungsprogramme diese Integration der Metadaten. Die auf diese Weise gespeicherten Metadaten des IIM werden häufig als *IPTC-Felder* oder *IPTC-Header* bezeichnet. Sie können in Bilddateien der Typen JPEG, TIFF und PNG gespeichert werden. Neben der Speicherung im Binärformat des IIM trat im Jahr 2004 die Speicherung der *IPTC-Metadaten* in Form von XMP. Das *IPTC-*

Core-Schema [63] bildet hierzu die Informationen des IIM in XMP ab und spezifiziert die Synchronisierung beider Datenformate. Mit dem *IPTC-Extension*-Schema wurden im Jahr 2008 weitere Kontextinformationen spezifiziert. IPTC-Core und IPTC-Extension bilden heute zusammen den *IPTC Photo Metadata Standard* [64] in der aktuellen Version aus dem Jahr 2010. Auf Basis von XMP können IPTC-Metadaten in einer Vielzahl von Bildformaten gespeichert werden.

2.3 Soziales Onlinenetzwerke und Foto-Communitys

Folgende Dienste des Social Webs wurden im Rahmen dieser Dissertation betrachtet und verwendet. Während es eine Vielzahl ähnlicher Dienste im Web gibt, können die hier betrachteten als stellvertretend für die meisten Dienste angesehen werden.

2.3.1 Facebook

Facebook ist ein Soziales Onlinenetzwerk, welches seinen Nutzern eine Vielzahl von Interaktionsmöglichkeiten bietet. Nutzer präsentieren sich gegenüber anderen Nutzern in Form ihres Online-Profils. Neben einem persönlichen Steckbrief können sie Fotos mit anderen Teilen oder persönliche Nachrichten austauschen. Im Rahmen ihrer *Chronik* (früher: *Pinnwand*) teilen Nutzer Informationen über ihr Leben oder schlichtweg ihre Meinung in Form von Statusmeldungen. Die Chronik dient auch der Verbreitung anderer Inhalte wie Bilder, Videos oder Weblinks. Ein Großteil der verbreiteten Inhalte kann von anderen kommentiert werden oder mit einem *gefällt mir* markiert werden. Über dies können sich die Nutzer wiederum informieren lassen, so dass eine komplexe Interaktion um die Inhalte entstehen kann.

Um den Kreis seiner Freunde und Bekannten im Soziales Onlinenetzwerk zu pflegen, führt jeder Nutzer eine Freundesliste. Für den gezielten Zugriff auf Informationen bestimmter Personengruppen können Listen zur Gruppierung von Personen erstellt werden. Das Füllen vorgegebener Listen wie *Familie*, *enge Freunde* und *Bekannte* und die Definition eigener Listen sind möglich. Diese Listen dienen ebenfalls der genaueren Festlegung von Zugriffsrechten für eigene Inhalte wie Fotos oder Statusmeldungen. So können Inhalte nur für den Nutzer selbst, *Freunde*, *Freunde ohne Bekannte* oder eine Kombination verschiedener Gruppen freigegeben werden.

Facebook bietet seinen Nutzern eine Vielzahl weiterer Funktionen, von denen nur einige hier vorgestellt werden. Gruppen dienen der offenen oder geschlossenen Kommunikation zu bestimmten Themen. Über *Orte* können Nutzer Anderen mitteilen, wo sie sich gerade aufhalten. Die Definition von Orten mit Namen und Beschreibungen gibt dabei genauere Informationen zu einer Vielzahl der angegebenen Orte. In diesem Zusammenhang können Geschäfte auch Rabattcoupons bei der Suche nach Orten in der Nähe anbieten. Die *Suche* erlaubte ursprünglich eine Suche nach Perso-

nennamen, Gruppen oder Orten. Inzwischen wurde sie zu einer semantischen Suche ausgebaut, die Suchanfragen wie „Fotos meiner Freunde, die in Nationalparks aufgenommen wurden“ ermöglichen soll.

Mit *Connect* bietet Facebook ein Single-Sign-On-System, das Nutzern erlaubt, sich mit ihrem Facebook-Login bei anderen Diensten anzumelden. Bisher bedeutete dies für einen Nutzer der Funktion, dass ein Teil seiner persönlichen Daten dem Dienstanbieter zugänglich wurde. Gleichzeitig nutzte Facebook die Informationen über genutzte Drittanbieter, wie viele andere gesammelte Daten, zur Personalisierung eingeblendeter Werbung. Seit Kurzem ist Facebook dabei einen anonymen Login für Drittangebote zu ermöglichen [13]. Facebook bietet anderen Dienstanbietern außerdem die Möglichkeit, ihr Angebot in Form von *Apps* in das Onlinenetzwerk zu integrieren. Solche Apps können dabei auf einen Großteil aller persönlichen Informationen, Fotos oder Nachrichten von Nutzer zugreifen, wenn sie die dazu jeweils notwendigen Berechtigungen durch die Nutzer erhalten. Auch der Zugriff auf Inhalte von Freunden kann Apps auf diese Weise ermöglicht werden. Durch den Zugriff auf persönliche Informationen können Apps ihr Angebot personalisieren, jedoch birgt die Nutzung persönlicher Informationen auch eine latente Bedrohung der Privatsphäre.

Facebook bietet verschiedene Einstellungen zum Schutz der Privatsphäre, mit deren Hilfe ein Nutzer den Zugriff auf seine eigenen Inhalte für Freunde, Fremde oder Apps beschränken kann. Nur ein Teil dieser Einstellungen ist unter den globalen Privatsphäre-Einstellungen zu finden. Andere sind häufig im Kontext der jeweiligen Funktion zu finden, wie beispielsweise die Sichtbarkeit der Freundesliste oder die Freigabe persönlicher Informationen an Apps, welche die eigenen Freunde nutzen.

Ursprünglich im Jahr 2004 für Studierende der Universität von Harvard entwickelt, ist Facebook seit September 2006 für alle Nutzer über 13 Jahren zugänglich. Mit monatlich bis zu 1,23 Milliarden aktiven Nutzern im Jahr 2013 ist Facebook das weltweit größte Soziales Onlinenetzwerk im Web. Bis zu 757 Million Nutzer hatte der Dienst im Jahr 2013 täglich, von denen fast drei Viertel mobile Nutzer waren [12]. Nur in einzelnen Ländern dominieren andere Soziale Onlinenetzwerke wie RenRen in China und VKontakte in Russland, die einen ähnlichen Funktionsumfang bieten. Bis September 2013 wurden bei Facebook 250 Milliarden Fotos hochgeladen. Der Dienst gab zu diesem Zeitpunkt an, dass täglich 350 Millionen weitere hinzukommen [61].

2.3.2 Flickr

Flickr ist eine Online-Community zum Teilen von privaten und semiprofessionellen Fotos sowie kurzen Videos. Der Dienst startete im Jahr 2004. Mit mehr als 8 Milliarden gehosteten Fotos ist die Foto-Plattform heute eine der führenden im Web. Dabei ist auch der Anteil von über 300 Millionen Fotos mit Geotags beachtlich.

Im Mai 2013 vermeldete Flickr 89 Millionen Nutzer. Zu diesem Zeitpunkt wurden

täglich mehr als 3,5 Millionen Fotos hochgeladen [53]. Durch eine grundlegende Erneuerung der Flickr-Webseite, durch die Auflösung vieler Beschränkungen der kostenfreien Nutzerkonten und durch die Veröffentlichung neuer Apps für Apple iOS und Android gewann Flickr ab Mai 2013 vermehrt neue Nutzer. Während die Neuerungen viele konservative Fotografen verärgerten, wurde das Zielpublikum der mobilen Nutzer verstärkt erschlossen. So berichtete Flickr 2013 von einem Zuwachs mobiler Nutzer um 50 % von Quartal zu Quartal. Die Flickr-App war zudem eine der mobilen Apps mit dem größten Nutzerzuwachs zwischen Q1/2013 und Q3/2013 [28]. Im Oktober 2013 waren die Nutzerzahlen entsprechend gestiegen: Flickr vermeldete 92 Millionen Nutzer und bis zu 10 Millionen neue Fotos pro Tag [52].

Im Vergleich zu anderen Diensten zum Teilen von Fotos setzt Flickr auf den aktiven Austausch über Fotos. Der Austausch findet mit privaten Kontakten statt und auch öffentlich, beispielsweise innerhalb der über 1,5 Millionen aktiven Themengruppen. Das Taggen von Bildern mit Schlagworten ist ein wichtiger Bestandteil von Flickr. Beim Durchstöbern von Fotos spielt das Konzept der Interestingness [59] eine wichtige Rolle. Neben einer detaillierten Rechtevergabe können Nutzer auch die Lizenz ihrer Bilder definieren. Im Oktober 2011 war Flickr mit 200 Millionen Fotos unter der Creative-Commons-Lizenz der größte Anbieter solcher Bilder.

Die meisten Funktionen des Dienstes, wie das Hochladen, das Ordnen oder das Suchen von Bildern oder die Abfrage von Informationen über Bilder und Nutzer, sind wie bei Facebook über eine öffentliche API zugänglich. Sie können so durch webbasierte Flickr-Apps oder andere Client-Anwendungen verwendet werden.

Flickr bietet seinen Nutzern unterschiedliche Mitgliedschaften an. Vor Mai 2013 konnten Nutzer zwischen zwei Arten von Nutzerkonten wählen: kostenfreie Konten und Pro-Mitgliedschaften in Form eines bezahlten Mehrwertdienstes. Nutzer der kostenlosen Konten waren begrenzt in Bezug auf die Anzahl, Größe und Frequenz des Hochladens von Bildern sowie der maximalen Anzahl an Fotos. Fotos wurden beim Hochladen verkleinert und nur der Zugriff auf die kleineren Versionen war möglich. Pro-Nutzer hatten nur eine Beschränkung für die maximale Dateigröße eines Fotos. Für die Webansicht wurden Fotos beim Hochladen ebenfalls verkleinert, jedoch wurde für Pro-Nutzer auch die Originaldatei erhalten und konnte auch anderen Nutzern zugänglich gemacht werden. Außerdem konnten Statistiken zu Bildern abgerufen werden und es wurden keine Werbebanner auf der Seite eingeblendet.

Seit Mai 2013 bietet Flickr seinen Nutzern drei Arten von Nutzerkonten: kostenfreie Konten, werbefreie Konten und mehr Speichervolumen. Seit dem Re-Design können Nutzer der kostenfreien Konten 1 TB Speicherplatz belegen, anstatt auf 200 Fotos begrenzt zu sein. Alle anderen Beschränkungen wurden weitestgehend aufgehoben. Auch für Nutzer der kostenfreien Accounts werden nun die Originaldateien erhalten und sie können allen Betrachtern zugänglich gemacht werden. Die Pro-

Mitgliedschaft wurde abgeschafft. Nutzer können sich stattdessen die Werbefreiheit oder mehr Speichervolumen erkaufen.

2.3.3 Locr

Locr ist eine auf Geotagging fokussierte Online-Community zum Teilen von Fotos. Neben dem Teilen von Fotos erlaubt der Dienst insbesondere das Erkunden von Fotos, die in der Umgebung anderer Fotos gemacht wurden.

2.3.4 Twitter

Twitter ist ein Mikroblogging-Dienst, der aufgrund seiner sozialen Komponenten auch als Soziales Onlinenetzwerk verstanden werden kann. Über kurze Blog-Beiträge teilen sich Twitter-Nutzer anderen Nutzern mit. Twitter-Nutzer verfolgen Beiträge anderer, während ihren wiederum andere Nutzer folgen. Auf diese Weise entsteht ein soziales Netzwerk, durch das Nachrichten ausgetauscht und weiterverbreitet werden. Die Kurznachrichten mit bis zu 140 Zeichen enthalten neben Text oft auch Weblinks zu anderen Seiten oder Fotos. Durch das Hinzufügen von Ortsinformationen zu Nachrichten können auch ortsgebundene Informationen geteilt und gefunden werden. Durch die sogenannten *Hashtags* werden häufig andere Metainformationen in die Kurznachrichten eingebunden.

2.4 Standortbezogene Dienste und Apps

Standortbezogene Dienste sind Dienste, die Standortinformationen für die Erbringung bereitgestellter Funktionen verwenden. Meist handelt es sich beim verwendeten Standort um den aktuellen Aufenthaltsort eines Nutzers. Heute existierende standortbezogene Dienste lassen sich in zwei Kategorien gliedern: Dienste, die standortbezogene Informationen oder Funktionen bereitstellen, und Dienste, die Standortinformationen von Nutzern verbreiten. Wenige Informationsdienste boten schon vor der Verbreitung von mobilen Geräten standortbezogene Informationen an. So konnten Nutzer auf einer Webseite beispielsweise die Restaurants in der Nähe einer vorgegebenen Adresse suchen. Ein Großteil der standortbezogenen Dienste entstand jedoch im Rahmen der massiven Verbreitung mobiler Geräte, die fähig sind, den aktuellen Aufenthaltsort ihres Nutzers zu bestimmen. Ein Großteil der Dienste wird heute auch im Form von Apps für die mobilen Geräte angeboten.

Informationsdienste Um Informationen zu einem Standort abzufragen, gibt ein Nutzer den gesuchten Ort in Form einer Adresse oder eines Stadtnamens ein oder er lässt seine Position vom verwendeten Gerät orten. Der auf die eine oder andere Weise bestimmte Ort wird daraufhin an einen Dienstanbieter übermittelt und der

Nutzer erhält Informationen mit Bezug auf den angegebenen Ort. Die Zahl und Vielfalt solcher Informationsdienste ist heute immens.

Beispielhafte Dienste und Apps:

- Diverse Wetter-Apps zeigen Wettervorhersagen und aktuelle Messwerte von Temperatur, Regen oder Wind zum Aufenthaltsort eines Nutzers an.
- *IMDb Filme & TV* zeigt einem Nutzer neben Informationen zu Filmen auch Informationen zum nächstgelegenen Kino und dessen aktuellen Programm.
- *Öffi - Fahrplanauskunft* zeigt einem Nutzer den Fahrplan und aktuelle Wartezeiten zu öffentlichen Verkehrsmitteln an umliegenden Haltestellen an.

Standortveröffentlichung Einige Dienste ermöglichen Nutzern, ihren aktuellen und zum Teil auch vergangenen Aufenthaltsort mit anderen Nutzern zu teilen. Dabei verwendet ein Teil der Dienste den genauen Ort des Nutzers in Form von Koordinaten. Dieser wird anderen meist auf einer Karte angezeigt. Andere Dienste definieren hingegen Orte in Form von Namen und Beschreibungen wie „Leibniz Universität Hannover“ oder „Mövenpick“ für die Angabe von Orten. Durch einen *Check-in* bei einem solchen Ort teilen Nutzer anderen mit, dass sie an diesem gewesen sind.

Beispielhafte Dienste und Apps:

- *Foursquare* (*Swarm*) bietet seinen Nutzern Informationen über Orte wie Cafés oder Kulturangebote in ihrer aktuellen Umgebung. Besucht ein Nutzer einen solchen Ort, kann er dort einchecken, so dass andere sehen, wann er an diesen Ort ist beziehungsweise war. Außerdem kann er seine Meinung oder Tipps zum besuchten Ort mit anderen teilen.
- *Glympse* ermöglicht einem Nutzer seinen aktuellen Aufenthaltsort mit beliebigen Personen für einen festgelegten Zeitraum zu teilen. Die Empfänger können die Bewegung des Nutzers über die App oder im Webbrowser verfolgen.

2.5 Beschreibung und Bestimmung von Orten

Ein Ort kann auf mehrere Weisen mit verschiedener Genauigkeit beschrieben werden.

Koordinaten beschreiben einen genauen Ort repräsentiert durch einen Punkt innerhalb eines Koordinatensystems. Komplexere Geoobjekte wie eine Straße oder ein Gebäude werden durch Linien und Flächen beschrieben, die beispielsweise durch eine Reihung von Punkten zu offenen und geschlossenen Linienzügen modelliert werden. Soll solch ein Objekt durch eine einzige Koordinate beschrieben werden, wird meist auf die Ermittlung des Mittelpunktes oder Schwerpunktes des Objektes zurückgegriffen. Außerdem können komplexere Objekte durch ein umschließendes Rechteck (Bounding Box) beschrieben werden, dessen Mittelpunkt ebenso als repräsentative

Ortsangabe verwendet wird. Wird nur eine Koordinate angegeben, kann ein äußerer Betrachter nicht zwischen einem genauen Punkt und einem repräsentativen Punkt unterscheiden. Beim Umgang mit Koordinaten darf nicht der Fehler gemacht werden, dass von der Zahl der Nachkommastellen auf die Genauigkeit einer Ortsangabe geschlossen wird.

Neben der Beschreibung durch Koordinaten können Orte auch durch Namen oder Adressen beschrieben werden. Der Name einer Sehenswürdigkeit reicht häufig aus, um einen Ort recht genau zu beschreiben. Eine Postadresse mit Straße und Hausnummer ist häufig ebenso genau wie Koordinaten, wenn man die technische Ungenauigkeit einer Ortung berücksichtigt. Werden Teile einer Adresse weggelassen, so verliert die Ortsangabe an Genauigkeit. Die Lagebeschreibung eines Ortes durch Koordinaten und die textuelle Beschreibung eines Ortes können auf Basis elektronischer Kartendaten meist durch Verfahren zur *Geokodierung* und *Adresskodierung* (umgekehrte Geokodierung) ineinander überführt werden.

Die Verarbeitung von Geoinformationen wird heute durch spezielle Datenbanksoftware erleichtert. Ein Beispiel bietet die PostGIS-Erweiterung für das freie Datenbankmanagementsystem PostgreSQL. PostGIS fügt spezielle Datentypen zur direkten Speicherung verschiedener Geometrien sowie Indexverfahren zu PostgreSQL hinzu. Außerdem wird die Abfrage von Geodaten vereinfacht, da performante Implementierungen für Funktionen wie beispielsweise Abstände oder Schnitte von Objekten integriert werden und auf diese in SQL-Anfragen zurückgegriffen werden kann.

2.5.1 Koordinatensysteme

Die Lage eines Punktes auf der Erde wird durch *geographische Koordinaten* beschrieben. Diese Koordinaten bezeichnen einen Punkt auf dem Gradnetz, einem gedachten Koordinatensystem auf der Erdoberfläche. Die Breitengrade verlaufen parallel zum Äquator (0. Breitengrad) und werden von diesem aus jeweils nach Norden und Süden bis zu den Polen (90. Breitengrad) gezählt. Von Pol zu Pol verlaufen senkrecht zu den Kreisen gleicher Breite die Längengrade (Meridiane). Der willkürlich festgelegte Nullmeridian liegt bei Greenwich in Großbritannien. Von diesem aus werden jeweils 180 Längengrade nach Osten und nach Westen gezählt. Geographische Koordinaten bestehen aus der geographischen Breite und Länge. Je nach Anwendungsgebiet werden die beiden Werte als Dezimalzahl ausgedrückt sowie durch die Angabe von Grad, Minuten und Sekunden gemäß des Sexagesimalsystems.

Da die Form unserer Erde eher einer Kartoffel als einer Kugel gleicht, wurden in der Vergangenheit für die Erde verschiedene Referenzsysteme (Körper und Lage) festgelegt, um Berechnungen zwischen Punkten anstellen zu können und die Erde möglichst korrekt auf Karten abzubilden. Das im Alltag wohl am häufigsten zugrunde liegende Referenzsystem ist das World Geodetic System 1984 (WGS-84), welches

die Grundlage für das Global Positioning System (GPS) darstellt. Es bestimmt das verwendete Rotationsellipsoid, ein Modell der Differenz zur realen Erdfigur und einen Satz von Koordinaten, die das Ellipsoid auf der Erde verankern.

Durch eine Kartenprojektion können die Informationen aus einem dreidimensionalen Referenzsystem auf eine zweidimensionale Karte projiziert werden. Je nachdem welcher Teil der Erde abgebildet wird und welchem Zweck eine Karte dient, wird eine passende Projektion verwendet, da die Abbildung einer Projektion spezifische Verzerrungen hervorruft. Im Rahmen dieser Dissertation wird das *UTM-Koordinatensystem* als Basis für Kartendarstellungen und Berechnungen verwendet. Das UTM-Koordinatensystem ist ein globales Koordinatensystem. Es teilt die Erde in mehrere Zonen, über die jeweils ein kartesisches Koordinatensystem gelegt wird. Ortsangaben innerhalb des Koordinatensystems werden durch einen Hochwert und einen Rechtswert in Metern angegeben. Für die im Rahmen dieser Dissertation betrachteten Flächen ist die Verzerrung so gering, dass die Wahl des Koordinatensystems erlaubt, Koordinatenbeziehungen durch einfache Geometrie in der Ebene genau zu bestimmen.

2.5.2 Geo- und Adresskodierung

Geokodierung bildet geographischen Daten wie eine Adresse oder den Namen einer Sehenswürdigkeit auf geographische Koordinaten ab. Die Kodierung läuft wie folgt ab: Mit den zu kodierenden Daten wird in einem geographischen Datenbestand nach passenden Geoobjekten, wie einer Straße, einem Gebäude oder einer Sehenswürdigkeiten gesucht. Wird ein passendes Objekt gefunden, oder ist bei mehreren Ergebnissen ein Objekt aus der Menge von Ergebnissen ausgewählt worden, so werden für dieses die Koordinaten bestimmt. Je nach Objekttyp des Ergebnisses wird die Koordinate direkt übernommen oder es wird der Mittelpunkt oder Schwerpunkt des Objektes selbst oder des umschließenden Rechtecks ermittelt. Alle gängigen Kartendienste im Web bieten eine Geokodierungsfunktion an. Listing 2.1 zeigt beispielhaft die Geokodierung von „Hauptmensa Hannover“ durchgeführt mit *Nominatim* auf Basis der Daten des *OpenStreetMap*-Projektes[1].

Listing 2.1: Geokodierung von „Hauptmensa Hannover“ (OpenStreetMap)

```
<place place_id="31368527" osm_type="way" osm_id
    ="16608589"
   boundingbox="52.385933,52.386845,9.713249,9.714528"
   polygonpoints="[...]" lat="52.386388" lon="9.713892"
   display_name="..." class="amenity" type="restaurant"
   place_rank="30" importance="0.301">
</place>
```

[1] Community-Projekt für frei nutzbare Geodaten und Karten: `http://www.openstreetmap.org/`

Adresskodierung bildet geographische Informationen wie geographische Koordinaten auf eine Adresse/Postanschrift ab. Mit gegebenen Koordinaten wird dazu eine Suche in einem Datenbestand geographischer Objekte durchgeführt. Eine triviale Implementierung sucht beispielsweise nach dem Geoobjekt mit dem geringsten Abstand zu den gegebenen Koordinaten, zu dem eine Adresse vorliegt. Die jeweilige Umsetzung ist unter anderem abhängig davon, wie ein System Adressen und Hausnummern speichert und welche Operationen (Abstand, Schnitt, etc.) für Anfragen zu Geoobjekten möglich sind. Listing 2.2 zeigt eine exemplarische Adresskodierung durchgeführt mit *Nominatim* auf Basis der Daten des OpenStreetMap-Projektes.

Listing 2.2: Adresskodierung von `N 52,38605° E 9,71394°` (OpenStreetMap)

```
<result place_id="31368527" osm_type="way" osm_id="16608589"
   ref="Hauptmensa" lat="52.3863886" lon="9.71389238462365">
 Hauptmensa, 23, Callinstraße, Nordstadt, Hannover,
 Region Hannover, Niedersachsen, 30167, Deutschland
</result>
<addressparts>
 <restaurant>Hauptmensa</restaurant>
 <house_number>23</house_number>
 <road>Callinstraße</road>
 <suburb>Nordstadt</suburb>
 <city>Hannover</city>
 <county>Region Hannover</county>
 <state>Niedersachsen</state>
 <postcode>30167</postcode>
 <country>Germany</country>
</addressparts>
</reversegeocode>
```

2.5.3 Weitere Begriffsdefinitionen

Geotagging bezeichnet das Anreichern von Inhalten mit Ortsinformationen. Durch die Georeferenzierung der Inhalte gibt der Ersteller eines Fotos oder der Autor eines Mikroblog-Beitrags oder einer Statusmeldung in einem Sozialen Onlinenetzwerk an, an welchem Ort ein Foto entstanden ist beziehungsweise wo sich der Autor zum Zeitpunkt des Schreibens und Veröffentlichen eines Beitrags befunden hat.

Das Vorhandensein einer ***geographischen Kollokation*** bedeutet, dass sich zwei Nutzer oder Geräte zeitweise in unmittelbarer Nähe zueinander befinden.

Der Begriff ***Verschleierung*** von Ortsinformationen umschreibt das kontrollierte Entfernen von Detail einer Ortsangabe. Zu diesem Zwecke können Koordinaten auf Basis entsprechender Verschleierungsmethoden verändert werden. Alternativ kann ein Ort durch weniger genaue Angaben beschrieben werden, wie beispielsweise durch den Namen der nächstgelegenen Stadt.

2.5.4 Methoden der Ortsbestimmung mobiler Geräte

Verschiedene Techniken erlauben heute, den Standort mobiler Geräte zu bestimmen. Mobilfunkanbieter haben verschiedene Möglichkeiten den Ort eines Mobilfunkgerätes zu bestimmen und bieten ihren Kunden dieses als Dienstleistung an, beispielsweise in Form von Handy-Ortung oder einer Kraftfahrzeug-Flotten-Management-Lösung. Viele mobile Geräte können zudem selbstständig oder auf Basis dritter Anbieter ihren eigenen Ort bestimmen. Satellitenbasierten Verfahren wie die GPS-Ortung bieten eine nahezu flächendeckende Ortsbestimmung, jedoch benötigen sie entsprechende Empfänger und verbrauchen durch diese zusätzlichen Strom. Im Ballungsgebieten unterliegen sie Einschränkungen aufgrund der Bebauung. Dort erzielt hingegen die WLAN-basierte Ortung oft eine hohe Genauigkeit.

Allgemein lassen sich verschiedene Methoden zur Ortsbestimmung unterscheiden. *Proximity Sensing* bezeichnet die Bestimmung eines Ortes durch die reine Nähe zu bekannten Referenzpunkten wie etwa Funkmasten. Ist der Abstand oder der Winkel von einem Punkt zu mehreren Referenzpunkten bekannt, so kann mittels *Lateration* oder *Angulation* die Bestimmung des Ortes im Referenzsystem über geometrische Berechnungen erfolgen. Liegt für lokale Phänomene, wie die Signalstärke umgebender Sender, ein hinreichender Datenbestand an Vergleichswerten vor, kann der Ort eines Empfängers anhand solcher *Fingerabdrücke* abgeschätzt werden.

2.5.4.1 Mobilfunk-Ortung

Sobald ein Mobilfunkgerät in ein Mobilfunknetz eingebucht ist, kann dessen Ort bestimmt werden. Die Genauigkeit der Ortung durch den Mobilfunkanbieter hängt dabei von der eingesetzten Technik ab. Beim Einbuchen eines Gerätes registriert der Netzbetreiber die ID der jeweiligen Funkzelle. Abhängig von der Dichte der Funkmasten kann so der Ort eines Gerätes mehr oder minder grob bestimmt werden, da die Orte der Basisstation bekannt sind. Für den Betrieb der Mobilfunkkommunikation wird die Signallaufzeit zwischen einem Funkmast und einem Endgerät bestimmt. Diese kann auch für die Bestimmung des Abstands der beiden herangezogen werden. In GSM-Netzen kann so beispielsweise vom Zeitmultiplex-Parameter Timing Advance auf die Entfernung zwischen Funkmast und Endgerät mit einer Auflösung von grob 550 Metern geschlossen werden. Auf Basis spezieller Positionierungskomponenten im Mobilfunknetz kann der Ort eines jeden Endgerätes weitaus genauer bestimmt werden. Durch die netzseitige Messung der Laufzeit bekannter Signale während einer aktiven Verbindung zwischen einem Gerät und mindestens drei solcher Komponenten kann so eine Genauigkeit im unteren zweistelligen Meterbereich erzielt werden. Auf den Endgeräten ist dazu keine weitere Hardware oder Software notwendig. Unter Einbeziehung eines Endgerätes kann außerdem über die Messung der Laufzeit von Signalen von mindestens drei Basisstationen der Ort des

Gerätes mit einer ähnlichen Genauigkeit bestimmt werden. Die Berechnung kann dabei im Netz oder auf dem Endgerät erfolgen, insofern diesem alle notwendigen Zusatzinformationen vorliegen. Mobilfunkstandards sehen außerdem vor, den Ort eines Endgerätes auch mittels satellitenbasierter Ortsbestimmung festzustellen. In diesem Fall bestimmen entsprechend ausgerüstete Mobilfunkgeräte ihren Ort mittels integrierter Hardware und teilen ihn dem Mobilfunknetz mit.

Neben der Ortsbestimmung durch die Mobilfunkanbieter ermöglichen heute auch dritte Anbieter den Nutzern moderner mobiler Geräte eine Ortsbestimmung auf Basis umgebender Funkmasten. Diese Angebote basieren auf eigenen Datenbanken und Algorithmen ohne Einbeziehung der Mobilfunkinfrastruktur. Ein Beispiel für solch ein Angebot bietet die *Google Maps Geolocation API*, die eine Bestimmung des Ortes eines Nutzers auch auf Basis der für sein Gerät sichtbaren Mobilfunkmasten anbietet. Für eigene Implementierungen bietet das Projekt OpenCellID hingegen eine kostenfreie community-basierte Kartierung von Mobilfunkzellen. Diese Art der mobilfunkbasierten Ortung wird auch von mobilen Betriebssystemen verwendet, welche nicht auf die Dienste der Mobilfunkanbieter zurückgreifen.

2.5.4.2 Satellitenbasierte Ortsbestimmung

Globale Navigationssatellitensysteme (GNSS) ermöglichen eine Ortsbestimmung durch den Empfang von Signalen von Navigationssatelliten. Das wohl bekannteste GNSS ist das *Global Positioning System* (GPS) der Vereinigten Staaten von Amerika. Aufgrund seiner langen Monopolstellung wird GPS oft synonym für GNSS verwendet. Weitere Systeme befinden sich heute jedoch im Aufbau: Galileo der Europäischen Union, GLONASS der Russischen Föderation und Compass aus China. Neben dedizierten GNSS-Empfängern und Navigationssystemen enthalten heute die meisten Smartphones einen entsprechenden Empfänger. Einige der integrierten Empfänger unterstützen sogar gleichzeitig mehrere Systeme wie GPS und GLONASS und ermöglichen so eine bessere Positionsbestimmung.

Während er die Erde umläuft, sendet jeder Satellit eines globalen Navigationssatellitensystems kontinuierlich einen individuellen Code sowie Daten zu seiner Umlaufbahn. Um seinen Ort zu bestimmen, sammelt ein Empfänger die Signale aller sichtbarer Navigationssatelliten. Für eine Ortsbestimmung muss der Empfänger die Signale von mindestens vier Satelliten gleichzeitig empfangen. Signale von mehr als vier Satelliten ermöglichen eine genauere Ortsbestimmung. Aus den empfangenen Daten ermittelt der Empfänger Entfernungen, so dass er auf Basis der Positionen und der Entfernungen der Satelliten seinen Ort mittels Lateration bestimmen kann.

Die Laufzeit der Satellitensignale wird durch die Erdatmosphäre beeinflusst, so dass die Genauigkeit des globalen Navigationssatellitensystems beeinträchtigt wird. Durchschnittliche private Empfänger ermöglichen eine Positionsbestimmung mit ei-

ner Genauigkeit zwischen 5 und 20 Metern. Die Genauigkeit kann jedoch mittels verschiedener technischer Methoden verbessert werden, die abhängig von der Position und der technischen Ausstattung eines Empfängers genutzt werden können. Mit diesen Korrektursystemen können Genauigkeiten von bis zu unter einem Meter erreicht werden. Beim differenziellen GPS werden über Langwellenfunk Korrekturdaten verbreitet, die durch ortsfeste Referenzempfänger eines GNSS berechnet werden. Diese Korrekturdaten beziehen sich auf den Punkt des Referenzsystems und ihre Genauigkeit nimmt daher mit der Entfernung zu diesem ab. Satellitenbasierte Ergänzungssysteme wie EGNOS senden Korrekturdaten über Satelliten. Die Daten enthalten ein Korrekturgitter für die vom System abgedeckte Fläche, das aus den Werten mehrerer Referenzempfänger berechnet wird. Diese Korrektur unterliegt so nicht der genannten Einschränkung des differentiellen GPS. Die Dauer einer initialen Positionsbestimmung kann bei Systemen wie dem GPS aufgrund des Systemdesigns bis zu über einer Minute dauern. Durch Hilfsinformationen wie dem ungefähren Ort des Empfängers oder einer Liste der aktuell sichtbaren Satelliten kann dies stark beschleunigt werden (Assisted GPS). Solche Informationen können auf Basis des Mobilfunknetzes oder über WLAN und das Internet bezogen werden.

2.5.4.3 WLAN-basierte Ortsbestimmung

Die WLAN-basierte Ortsbestimmung macht sich die Existenz der Vielzahl kommerzieller WLAN-Hotspots und privater WLAN-Access-Points zunutze, um die Position eines WLAN-Gerätes zu ermitteln. Da die Genauigkeit der Ortsbestimmung direkt mit der Anzahl der umliegenden Access Points in Zusammenhang steht, ist diese Art der Ortung besonders in Ballungsgebieten effektiv. Innerhalb von Gebäuden ist WLAN-basierte Ortsbestimmung häufig genauer als mobilfunkbasierte oder satellitenbasierte Ortsbestimmung und dient heute auch als Basis für Indoor-Navigationssysteme. Um den Ort auf Basis von Access Points bestimmen zu können, müssen diese vorerst kartiert werden, so dass die Positionen dieser Referenzpunkte bekannt sind. Neben freien Projekten zur Kartierung wie der *OpenWLANMap*, gibt es kommerzielle Angebote für die Ortung, wie die der Firma Skyhook Wireless, auf denen anfangs die WLAN-basierten Ortungsdienste des Apple iPhones basierten. Die Marktführer im Bereich Smartphones und Tablets Apple und Google besitzen heute eigene Access-Point-Datenbanken und darauf aufbauende Dienste. Die Nutzer dieser Dienste sorgen dabei selbst für die Aktualisierung des Datenbestands, indem sie nicht nur Daten des Dienstes nutzen, sondern auch aktuelle Daten sichtbarer Access Points an die Anbieter zurück melden.

Die Ortsbestimmung kann auf verschiedene Weisen geschehen. Die erste Näherung an den Ort eines Endgerätes ist der Ort eines Access Points, mit dem das Gerät verbunden ist. Dies ist vergleichbar mit der Funkzellenermittlung im Mobilfunknetz.

Die Genauigkeit dieser Methode ist ungewiss, da die Größe einer WLAN-Zelle abhängig von der Umgebung stark variieren kann: grob bis zu 200 Meter auf freiem Feld und zwischen 50 und 10 Metern in Gebäuden. Genauer kann der Ort in der Regel auf Basis empfangener Signale von mehreren Access Points bestimmt werden. Neben der Liste sichtbarer Access Points stehen für die Ortsbestimmung die Signalstärke empfangener Signale und der jeweilige Rauschabstand zur Verfügung, die als grobes Maß für den Abstand zwischen Sender und Empfänger verwendet werden können. Je nach Umsetzung kann die Positionierung durch den Vergleich mit einzelnen Referenzpunkten geschehen oder durch den Vergleich mit einem auf Referenzmessungen basierenden Modell. Aufgrund der Abhängigkeit des Vergleichsverfahrens und der Anzahl umgebender Access Points kann keine allgemeine Genauigkeit für die WLAN-basierte Ortsbestimmung angegeben werden. Im Idealfall kann diese bis unter 20 Meter betragen. Skyhook Wireless gibt für seine Dienste sogar eine Genauigkeit von 10 Metern an. Methoden auf Basis von Signallaufzeiten kommen bei WLAN-basierter Ortung nicht in Betracht, da keine exakten Uhreinstellungen beziehungsweise keine Zeitsynchronität der beteiligten Geräte vorausgesetzt werden kann, die für die angestrebte Genauigkeit von Nöten wäre.

2.5.4.4 Bluetooth-basierte Ortsbestimmung

Die Funktechnologie Bluetooth ermöglicht ebenfalls eine Ortsbestimmung. Mit iBeacon führte die Firma Apple im Jahr 2013 einen Standard für die Navigation in geschlossenen Räumen ein, der auf Bluetooth Low Energy basiert. Die Ortung auf Basis von iBeacon-Sendern wird von Apples iOS 7 und Android 4.3 unterstützt. Durch Proximity Sensing oder Lateration kann ein Gerät seinen Ort relativ zu den sichtbaren Sendern feststellen. Ist der Ort der Sender bekannt, kann auch der Ort eines Endgerätes über ein Gebäude hinaus festgestellt werden.

2.5.5 Zugriff auf Standortinformationen mobiler Geräte

Die mobilen Betriebssysteme Apple iOS und Android ermöglichen Apps den Zugriff auf Standortinformationen von Geräten, auf denen diese installiert werden. Abhängig vom Betriebssystem können die Nutzer dabei die Verwendung ihres Standortes verschieden beeinflussen. Die mobilen Systeme haben gemeinsam, dass die Nutzung der Informationen zentral für alle Anwendungen erlaubt oder verboten werden kann.

2.5.5.1 Apple iOS

Apple iOS ermöglicht seinen Nutzern seit Version 6, den Zugriff auf Standortinformationen, die *Ortungsdienste*, für jede App einzeln zu steuern. Auf diese Weise können die Nutzer standortbezogene Apps nutzen, ohne allen Apps den Zugriff ein-

räumen zu müssen. Greift eine App erstmals auf die Standortinformationen zu, so öffnet sich ein Pop-up-Dialog, der den Nutzer fragt, ob er der App den Zugriff gewähren möchte. Die gewählte Einstellung gilt von diesem Zeitpunkt an für die App, bis der Nutzer sie in den Einstellungen ändert. Entwickler können im beschriebenen Pop-up-Dialog einen Zweck für die Nutzung der Ortsinformationen angeben. In der Praxis wird dies jedoch kaum verwendet. Benötigt eine App genaue Ortsinformationen eines GPS-Empfängers, so können die Entwickler dies in den App-Metadaten festlegen. In diesem Fall wird die App in Apples App Store nur für solche Geräte angeboten, die einen GPS-Empfänger integrieren.

2.5.5.2 Android

Android ermöglicht bis dato nur die Nutzung von Standortinformationen, den *Standortzugriff*, zentral zu deaktivieren. Einstellungen für einzelne Apps können nicht getätigt werden. Nutzer von Android können hingegen bestimmen, ob alle ihre Apps genaue Standortinformationen basierend auf allen Ortungstechniken inklusive GPS-Ortung erhalten, oder ob sie nur grobe Ortsangaben aus Basis der WLAN- und mobilfunkbasierten Ortung erhalten. Für den Zugriff auf den aktuellen Aufenthaltsort benötigt eine App die entsprechende Berechtigung für den Zugriff auf grobe oder genaue Ortsinformationen. Die Notwendigkeit der Berechtigungen bestimmen die Entwickler einer App. Will ein Nutzer eine App installieren, muss er alle geforderten Berechtigungen akzeptieren. Ein Einschränken oder Entziehen einzelner geforderter Berechtigungen erlaubt Android nicht. Will ein Nutzer die geforderten Rechte einer App nicht akzeptieren, bleibt ihm nur die App nicht zu installieren.

2.6 Privatsphäre

Für den Begriff der Privatsphäre (englisch: *Privacy)* existiert keine konstante und einheitliche Definition. Historisch gewachsene, kulturelle und kontextuelle Unterschiede sorgen unter anderem dafür, dass das Verständnis und die Umsetzung des Konzepts Privatsphäre recht unterschiedlich sind. Privatsphäre kann einerseits die Abgrenzung des Persönlichen vor staatlichem Einwirken meinen, jedoch ebenso die ganz persönliche Grenzziehung zwischen Individuen.

Schon der Philosoph Aristoteles trennte in der Antike die politische und häusliche Sphäre durch die Differenzierung der Polis und der Oikos [87]. Selbst wenig entwickelte Naturvölker zeigen mit dem Tragen eines Feigenblatts, dass auch sie ein gewisses Minimum an Schutz persönlicher Räume kennen. Der Schutz der Privatsphäre des Individuums als ein Recht in der modernen Gesellschaft ist jedoch ein relativ junges Konzept, dessen Ursprung der westlichen Kultur zugeschrieben wird. Die Entwicklung des Rechtsstaats, der Persönlichkeitsrechte und schließlich

die Idee der Selbstbestimmung legten etwa zur Zeit der Französischen Revolution den Grundstein für das heutige, hier zugrunde liegende Verständnis der Privatsphäre. Die Entwicklung des heutigen Lebensstandards mit einer eigenen Wohnung und separaten Zimmern und die Entwicklung der Technik mit Zeitungsdruck, Fotografie und Neuen Medien haben verschiedene private Schutzbereiche entstehen lassen.

Eine einfache und grundlegende Definition der Privatsphäre lieferten Warren und Brandeis im Jahr 1890 in ihrem Harvard Law Review als das „Recht, in Ruhe gelassen zu werden“ [147]. Sie verstehen Privatsphäre somit als für sich sein zu können ohne eine Einmischung anderer. Eine insbesondere in den Kontext der Informationstechnik passende Definition lieferte Westin im Jahr 1967 durch die Beschreibung von Privatsphäre als „den Anspruch, selbst zu bestimmen, wann, wie und in welchem Ausmaße persönliche Informationen anderen gegenüber kommuniziert werden“ [148]. Westin konzentriert sich damit auf den Aspekt der Kontrolle persönlicher Informationen. Wird im Rahmen dieser Dissertation der Begriff der Privatsphäre gebraucht, so ist dieser wie folgt zu verstehen:

> Die ***Privatsphäre*** einer Person ist der nicht-öffentliche Bereich, in dem die Person autonom und somit unbehelligt von äußeren Einflüssen der freien Entfaltung ihrer Persönlichkeit nachgehen kann. Dieser Bereich beschränkt sich nicht auf materielle Räume wie ihre eigene Wohnung, sondern umfasst auch andere Orte, in denen die Person beispielsweise ihre Freizeit verbringt, sowie auch immaterielle Räume, wie ihre eigene Gedankenwelt oder zum Beispiel auch Orte innerhalb des World Wide Webs. Die Wahrung ihrer Privatsphäre umfasst das Recht, in Ruhe gelassen zu werden und ungestört persönlichen Dingen nachgehen zu können, jedoch ebenso die autonome Bestimmung der Verbreitung und Verwendung persönlicher/personenbezogener Informationen, um diese innerhalb ihrer eigenen Privatsphäre zu halten.

Da sich die im Rahmen dieser Dissertation präsentieren Ansätze und Ergebnisse vorwiegend auf das Bewusstsein der Nutzer und die Selbstkontrolle durch diese fokussieren, sind rechtliche Regelung des Schutzes der Privatsphäre und der Datenschutz hier nicht von zentraler Bedeutung. Der rechtliche Rahmen, in dem sich die Nutzer bewegen, wird daher im Folgenden nur grob skizziert.

2.6.1 Rechtsgrundlagen

Der Schutz der Privatsphäre wird im deutschen Recht aus dem *allgemeinen Persönlichkeitsrecht* abgeleitet, welches ein absolutes umfassendes Recht auf Achtung und Entfaltung der Persönlichkeit ist. Dieses Recht ist selbst nicht im Grundgesetz (GG) definiert. Das allgemeine Persönlichkeitsrecht wurde seit 1954 mit einer Vielzahl von Entscheidungen zum Persönlichkeitsschutz in richterlicher Rechtsfortbildung von Artikel 2 Absatz 1 GG (*Freie Entfaltung der Persönlichkeit*) in Verbin-

dung mit Artikel 1 Absatz 1 GG (*Schutz der Menschenwürde*) abgeleitet. Heute ist es in der allgemeinen Rechtsüberzeugung als Gewohnheitsrecht anerkannt.

Um die Zulässigkeit des Eindringens in den persönlichen Bereich einer Person besser beurteilen zu können, wird im Rahmen der Sphärentheorie der durch das allgemeine Persönlichkeitsrecht geschützte Bereich in Sphären unterschiedlicher Schutzintensität unterteilt:

1. Die *Sozialsphäre* (*Individualsphäre*) umfasst die Bereiche, in denen eine Person mit anderen Personen der Gesellschaft agiert. Auf Basis geltenden Rechts darf in diese Sphäre eingegriffen werden.
2. Die *Privatsphäre* umfasst das Privatleben im häuslichen Bereich und der Familie, sowie auch andere einzelne Ereignisse mit privatem Charakter. Eingriffe in sie unterliegen dem Verhältnismäßigkeitsgrundsatz.
3. Die *Intimsphäre* umfasst die innere Gedankenwelt, die Gefühlswelt sowie den Sexualbereich. Sie ist grundsätzlich dem staatlichen Zugriff verschlossen.

Weitere Regelungen bestimmen über das allgemeine Persönlichkeitsrecht hinaus den Schutz der Privatsphäre. Das Grundrecht auf *Unverletzlichkeit der Wohnung* (Artikel 13 Absatz 1 GG) schützt die räumliche Privatsphäre in der eignen Wohnung, jedoch auch in anderen Räumlichkeiten, die je nach Zweck verschiedene Schutzintensitäten genießen. Das *Telekommunikationsgeheimnis* (Artikel 10 Absatz 1 GG) schützt den Inhalt wie auch die Metadaten der Kommunikation von Personen. Die Speicherung von Verbindungsdaten sowie anderer personenbezogener Informationen wird durch das Grundrecht auf *informationelle Selbstbestimmung* geschützt. Dieses Grundrecht wurde im Jahr 1983 mit dem „Volkszählungsurteil“ des Bundesverfassungsgerichts für Recht erkannt. Das Recht gewährleistet natürlichen Personen, selbst über die Preisgabe und Verwendung ihrer eigenen personenbezogenen Daten zu entscheiden. Das Volkszählungsurteil hatte insbesondere Einfluss auf das *Bundesdatenschutzgesetz* aus dem Jahr 1990 und die *Landesdatenschutzgesetze*. Diese formulieren Regelungen zum Schutz personenbezogener Daten, die manuell und durch Informations- und Kommunikationssysteme verarbeitet werden. Über die Datenschutzgesetze hinaus formulieren andere Gesetze wie beispielsweise das Telekommunikationsgesetz oder das Telemediengesetz weitere Regelungen zum Schutz personenbezogener Daten.

2.6.1.1 Recht am eigenen Bild

Das *Recht am eigenen Bild* (*Bildnisrecht*) regelt das Bestimmungsrecht von Personen über die Verbreitung und Veröffentlichung von Bildern ihrer selbst. Das Recht ist eine besondere Ausprägung des allgemeinen Persönlichkeitsrechts. Es ist ausdrücklich

gesetzlich geregelt im *Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie* (Kunsturheberrechtsgesetz) aus dem Jahr 1907.

2.6.1.2 Internationaler Vergleich

International existiert eine Vielzahl von Richtlinien und Regelungen, beispielsweise in Form der *Allgemeinen Erklärung der Menschenrechte* der Vereinten Nationen, der UN-Resolution zum *Recht auf Privatheit im digitalen Zeitalter* oder der *Europäischen Datenschutzkonvention*. Der Schutz der Privatsphäre und – im Hinblick auf die Informationstechnik von besonderer Bedeutung – der Schutz personenbezogener Daten ist im nationalen Recht anderer Länder häufig weniger ausgeprägt als in Deutschland.

2.6.2 Weitere Begriffsdefinitionen

Ist eine Sache/eine Information ***privat***, so bedeutet dies, dass sie nicht öffentlich ist beziehungsweise nicht für die Öffentlichkeit bestimmt ist. Vielmehr ist sie nur für eine einzelne Person bestimmt oder für eine abgegrenzte Gruppe von Personen, die untereinander in einem bekannten Vertrauensverhältnis stehen. Die Entscheidung, ob etwas privat ist, obliegt dem Besitzer des Privaten beziehungsweise der oder den durch eine Information betroffenen Personen.

Eine Person entscheidet für sich, ob eine bestimmte, persönliche oder personenbezogene Information im Rahmen ihrer eigenen Einschätzung und Entscheidung privat ist oder nicht. Sie entscheidet somit über die ***Privatheit*** der Information.

Den Begriff der ***personenbezogenen Daten*** definiert das deutsche Bundesdatenschutzgesetz als „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“. Solche Daten umfassen alle Informationen, die sich direkt auf eine Person beziehen oder über weitere Schlüsse auf eine Person beziehbar sind. Viele im Rahmen dieser Dissertation betrachtete Informationen, die die Privatsphäre einer Person bedrohen können, sind personenbezogene Daten. Teilweise können Informationen, wie beispielsweise der Titel oder die Beschreibung eines Bildes, auch nur persönlich (im Sinne von eigen) sein und keinen Personenbezug zulassen. Da diese Differenzierung vom Einzelfall abhängt, wird im Verlauf dieser Dissertation vorwiegend von persönlichen Informationen gesprochen, auch wenn es sich teilweise um personenbezogene Daten handeln könnte.

2.6.3 Privacy Segmentation nach Westin

Als einer der Pioniere im Bereich der Verbraucherprivatsphäre führte Westin ab den späten 1970er-Jahren über 30 Studien zur Privatsphäre durch. Die Studien befassten sich unter anderem mit Privatsphäre im Allgemeinen sowie mit der Wahrnehmung

der Menschen wie Firmen mit persönlichen Daten von Verbrauchern umgehen. Im Rahmen der Studien erstellte Westin Privatsphären-Indexe [120], die der Zusammenfassung seiner Ergebnisse dienten, die jedoch auch von anderen Wissenschaftlern verwendet werden, um Studienergebnisse beziehungsweise Teilnehmer zu klassifizieren und Stichproben zu charakterisieren und zu vergleichen. Der in der Studie „Privacy On and Off the Internet: What Consumers Want“ [149] beschriebene *Privacy Segmentation Index* (auch: *Core Privacy Orientation Index*) aus dem Jahr 2001 wird so in einer Vielzahl wissenschaftlicher Arbeiten zur Privatsphäre im Internet wie auch für Studien im Rahmen dieser Dissertation herangezogen, um Studienteilnehmer und die gewählten Stichproben zu beurteilen. Gemäß Westins Indexes teilt sich die amerikanische Bevölkerung in drei Privatsphäre-Klassen: *Fundamentalisten*, *Unbekümmerte* und *Pragmatisten*.

Privatsphäre-Fundamentalisten ordnen der Privatsphäre einen besonders hohen Stellenwert zu und lehnen die Erfassung von persönlichen Daten durch Organisationen oder für staatliche Programme ab. Sie sind der Meinung das mehr Menschen die Herausgabe von Informationen ablehnen sollten und sind für strenge gesetzliche Regelungen zum Schutz der Privatsphäre.

Privatsphäre-Unbekümmerte wissen nicht, was alles hinter dem „Aufheben um Privatsphäre“ steckt. Sie ziehen die Vorzüge von Angeboten auf Basis persönlicher Informationen den Warnungen über deren Missbrauch vor. Sie haben keine Scheu ihre persönlichen Informationen mit Firmen oder Regierungsorganisationen zu teilen und sehen keine Erfordernis weiterer Regelungen zum Schutz der Privatsphäre.

Privatsphäre-Pragmatisten wägen für sich selbst und die Gesellschaft den Wert einer gebotenen Leistung einer Firma oder der Regierung gegen preiszugebende persönliche Informationen ab. Auf Basis der Relevanz persönlicher Informationen, potenziellen Risiken für die Sicherheit dieser oder ihrer Privatsphäre und der Angemessenheit der Informationsnutzung entscheiden sie von Fall zu Fall. Das Vertrauen in den jeweiligen Leistungsanbieter ist ein wichtiger Entscheidungsfaktor. Pragmatisten bevorzugen die freiwillige Reglementierung und die Mitbestimmung durch den Nutzer gegenüber rechtlichen Regelungen, außer sie sehen einvernehmliche Regelungen als nicht ausreichend an.

Da Westins Erhebungen für die amerikanische Bevölkerung durchgeführt wurden und sich die Wahrnehmung von Privatsphäre zwischen Ländern wie den USA und Deutschland unterscheidet, sind die Zahlenwerte der Anteile der drei Klassen aus Westins Studien nur eingeschränkt für einen direkten Vergleich mit deutschen Teilnehmern geeignet. Die Klassifizierung kann jedoch uneingeschränkt zur Charakterisierung von Stichproben herangezogen werden.

Für die Erhebung der Wahrnehmung von Privatsphäre von Teilnehmern durch den beschriebenen Privatsphären-Index werden Teilnehmern drei Aussagen präsen-

tiert, die jeweils mit einer der folgenden Antworten bewerten werden: *stimme überhaupt nicht zu*, *stimme eher nicht zu*, *stimme eher zu* oder *stimme voll zu*.

(1) Verbraucher haben jegliche Kontrolle über die Erfassung und Verwendung von persönlichen Daten durch Firmen verloren.

(2) Die meisten Firmen behandeln die persönlichen Daten, die sie von Verbrauchern erfassen, angemessen und vertraulich.

(3) Bestehende Gesetze und Geschäftspraktiken bieten heute angemessenen Schutz für die Privatsphäre der Verbraucher.

Auf Basis der Antworten erfolgt die Klassifizierung der Person: Fundamentalisten sind diejenigen, die zu (1) voll/eher zustimmen und zu (2) und (3) eher/überhaupt nicht zustimmen. Unbekümmerte sind diejenigen, die zu (1) überhaupt/eher nicht zustimmen und zu (2) und (3) eher/voll zustimmen. Pragmatisten sind alle übrigen.

2.7 Bewusstsein

Gemäß Duden[2] ist ***Bewusstsein***

1. (a) der Zustand, in dem man sich einer Sache bewusst ist; deutliches Wissen von etwas, Gewissheit.
   (b) die Gesamtheit der Überzeugungen eines Menschen, die von ihm bewusst vertreten werden.
   (c) die Gesamtheit aller jener psychischen Vorgänge, durch die sich der Mensch der Außenwelt und seiner selbst bewusst wird (Psychologie).
2. der Zustand geistiger Klarheit; volle Herrschaft über seine Sinne.

Im Rahmen dieser Dissertation wird der Begriff entsprechend der Definition 1a des Dudens verstanden: Das Bewusstsein oder sich bewusst sein bedeutet zuallererst ein deutliches Wissen über etwas haben. Dieses Wissen erlaubt im Weiteren informiertes beziehungsweise bewusstes Handeln.

Bewusstsein und Privatsphäre

Die Schaffung von Bewusstsein in Bezug auf die eigene Privatsphäre und deren Wahrung gegenüber Bedrohungen im Kontext von IT-Systemen findet in zweierlei Form statt.

Eine Aufklärung über die Existenz und die mögliche Verwendung persönlicher Informationen stellt die grundlegende Form der Schaffung von Bewusstsein dar. Sie

[2] Duden online: `http://www.duden.de/rechtschreibung/Bewusstsein` am 14.02.2014, Bibliographisches Institut GmbH, 2013.

findet idealerweise schon im Vorfeld der Benutzung technischer Systeme statt. Diese fundamentale Aufklärung kann und sollte im Rahmen der Erziehung oder im Rahmen der Ausbildung stattfinden. Im deutschen Schulsystem wäre dies beispielsweise ein Aspekt der Vermittlung von Medienkompetenz.

Ein allgemeines, grundlegendes Bewusstsein hilft in der Praxis im Umgang mit der Vielfalt der heutigen Systeme jedoch nur eingeschränkt. Vielmehr muss über die Aufklärung hinaus Bewusstsein geschaffen werden, wie und wann die Privatsphäre eines Nutzers im Einzelfall bedroht werden könnte. In den einzelnen Anwendungsfällen muss dazu Wissen über die verwendeten persönlichen Informationen und deren Verbreitung erzeugt werden. Zuerst muss Bewusstsein geschaffen werden, dass Informationen vorhanden sind. Darüber hinaus muss Transparenz hergestellt werden: Den Nutzern soll Einsicht in die verwendeten Informationen ermöglicht werden. Dies kann auf technischem Wege beispielsweise durch Softwarewerkzeuge ermöglicht werden. Diese können im jeweiligen Anwendungsfall Informationen für einen Nutzer aufbereiten und bereitstellen, damit er vollkommen bewusst mit seinen Informationen umgehen kann. Bei unwissenden Personen helfen solche technischen Lösungen außerdem der Aufklärung: Durch die Konfrontation der Nutzer mit unbewusst genutzten persönlichen Informationen kann ihr Unwissen verringert werden.

Erst auf die Schaffung von Bewusstsein kann schließlich informiertes Handeln folgen und Kontrolle über persönliche Informationen ausgeübt werden.

Kapitel 3

Verwandte Arbeiten

Dieses Kapitel umreißt andere Arbeiten im Themenfeld dieser Dissertation. Zuerst werden Arbeiten zum Bewusstsein über die Preisgabe persönlicher Informationen vorgestellt. Anschließend werden verwandte Arbeiten zu den betrachteten Anwendungsfällen Bilder und Metadaten im Web und Standortinformationen präsentiert.

3.1 Schaffung von Bewusstsein

Die Schaffung von Bewusstsein wurde in verschiedenen Bereichen betrachtet.

3.1.1 Privatsphäre

Pötzsch [131] präsentierte basierend auf den Definitionen von Privacy nach Westin, Warren und Brandeis eine grundlegende Definition von *Privacy Awareness*, die dem Verständnis des Bewusstseins über die Preisgabe von persönlichen Informationen dieser Dissertation nahekommt: Sie definiert diese als Wahrnehmung und Wissen darüber, ob Andere persönliche Informationen erlangen, welche Information sie erlangen und wie sie diese verarbeiten und nutzen. Die Autorin fokussiert sich auf die Anwendungsfälle E-Commerce und Web-Communitys. In ihrer Arbeit beschreibt sie den häufig identifizierten Widerspruch, dass die Nutzer ihre Daten im Web preisgeben, auch wenn sie den Anspruch erheben, ihre Privatsphäre schützen zu wollen. Dieses „Privatsphäre-Paradoxon“ begründet sie mit der Kosten-Nutzen-Abschätzung, die viele Nutzer häufig situationsabhängig machen und dabei ihren persönlichen Vorteil gegen die Preisgabe persönlicher Information abwägen. Als ein Problem beschreibt die Autorin, dass vielen Nutzern nicht klar sei, wer alles Teil des Publikums im Web sein kann, welches Zugriff auf ihre Informationen hat. Als Lösungsansätze beschreibt Pötzsch, die Nutzer in Entscheidungssituationen an ihre eigene Einstellung zur Privatsphäre zu erinnern und ihnen klar zu machen, wer alles Empfänger ihrer Informationen sein könnte. Diese Dissertation fokussiert sich im Vergleich zu

Pötzschs Arbeit auf die Informationen selbst, um Nutzern eine fundierte, bewusste Preisgabe oder Nicht-Preisgabe der Daten zu ermöglichen.

Kagal und Abelson [114] kritisieren das generelle Vorgehen zum Schutz der Privatsphäre im Web: Zugriffsschutzmechanismen seien kein adäquates Mittel, um die Privatsphäre zu schützen. Die Autoren beschreiben alternative Wege, die sich an rechtlichen und sozialen Regeln des realen Lebens orientieren, wo der Privatsphäreschutz meist besser funktioniere: Webangebote müssten rechtzeitig über Datensammlung informieren, so dass Nutzer entsprechend reagieren können. Die Nutzung und Weitergabe von Informationen sollte rückverfolgbar sein, um einen Missbrauch unwahrscheinlicher zu machen, weil in diesem Fall nachgewiesen werden könnte, wer ein Täter gewesen ist. Nutzerschnittstellen müssten Nutzern deutlich zeigen, wann sie mit Daten anderer Personen agieren, um ihnen zu ermöglichen mit diesen respektabel umzugehen. Die Nutzer müssten zudem Richtlinien für den Umgang mit ihren Daten definieren können und diese anderen gegenüber kommunizieren können.

Im Kontext des klassischen Webs wurde der Fokus von Arbeiten zu Privacy Awareness hauptsächlich auf zwei Aspekte gerichtet: die Selbstauskunft von Anbietern und die aktive Überwachung der Informationspreisgabe durch die Nutzer.

Selbstauskunft der Anbieter Ein Web-Standard, der im Kontext der Selbstauskunft zu nennen ist, ist *Platform for Privacy Preferences* (P3P) des WWW Consortiums aus dem Jahr 2002. Das Ziel von P3P war, Nutzern zu ermöglichen, auf standardisiertem Wege Informationen zur Erfassung, Speicherung und Verwendung ihrer persönlichen Informationen durch Webseiten-Anbieter zu erlangen. Hierzu definiert der Anbieter einer Webseite ein maschinenlesbares P3P-Profil und hinterlegt es zum Abruf durch einen Webbrowser/P3P-Agenten. Dieser zeigt dem Nutzer die Informationen beim Besuch der Seite in einer verständlichen Weise an. Der Nutzer muss in diesem Fall der Selbstauskunft darauf vertrauen, dass die Webseiten-Betreiber vollständige und wahrheitsgetreue Angaben in ihren P3P-Profilen machen.

Cranor et al. [86] evaluierten im Jahr 2002 den P3P-Agenten *Privacy Bird*, der auch die Privatsphäre-Vorstellungen seiner Nutzer miteinbezieht. Nutzer von Privacy Bird legen in der Browser-Erweiterung ihre persönlichen Privatsphäre-Präferenzen fest, welche beim Besuchen von Webseiten mit den jeweiligen P3P-Profilen verglichen werden. Durch visuelles und akustisches Feedback wird dem Nutzer die Übereinstimmung oder Abweichung vom P3P-Profil und seinen Präferenzen angezeigt. Über eine Detailansicht kann er sich die Abweichungen anzeigen lassen. Die Studie zeigte, dass die Verwendung der Browser-Erweiterung viele Nutzer dazu brachte, sich vermehrt mit Datenschutzerklärungen zu befassen. Sie führte zu einem bewussteren Umgang mit dem Thema Privatsphäre.

In einer späteren Veröffentlichung [85] diskutierte Cranor die Entwicklung, Kritikpunkte und Schwachstellen des P3P-Ansatzes der vergangenen Jahre. Gemäß ih-

rer Analyse hat sich P3P über die Jahre zu einem nutzlosen Standard entwickelt. Dies ist unter anderem damit zu begründen, dass es keine externe Kontrolle gibt, ob Profile wahrheitsgetreu erstellt werden. Die Autorin weist darauf hin, dass viele Webseiten – wie auch Google oder Facebook – heute P3P vorwiegend umsetzen, um einer Cookie-Blockade im Microsoft Internet Explorer zu entgehen, der als einziger weitverbreiteter Webbrowser den P3P-Standard unterstützt.

Cranor, Egelman et al. [89, 85] präsentierten *Privacy Finder*, eine Suchmaschine, die P3P-Informationen auswertet und zusammen mit den Suchergebnissen eine Privatsphäre-Bewertung der einzelnen Webangebote anzeigt. Ein grüner Balken zeigt den Nutzern an, wie gut eine Webseite ihre persönlichen Daten schützen soll.

In ihrer Arbeit fasst Cranor [85] weitere Maßnahmen zur Selbstauskunft zusammen, die Bewusstsein über verwendete Informationen schaffen können: Angelehnt an Nährwertangaben auf Lebensmittelverpackungen kann eine „Privatsphäre-Nährwerttabelle“ über die Verwendung persönlicher Daten Auskunft geben. Verschiedene Hinweis-Icons, wie die *Know Privacy Icons* und die *Mozilla Privacy Icons*, wurden in der Vergangenheit entwickelt, die den Umgang mit persönlichen Daten auf Webseiten symbolisch darstellen sollen. Solche Methoden können nicht generell dem Schutz der Privatsphäre aller Nutzer dienen, sie können jedoch interessierten Nutzern schneller Auskunft geben, als es textuelle Datenschutzerklärungen tun.

Überwachung aufseiten der Nutzer Malandrino et al. [125] erweiterten die zuvor genannte Definition von Privacy Awareness um das Wer und Wann der Informationserfassung. Mit *NoTrace* präsentierten sie eine Browser-Erweiterung, die Nutzer beim Surfen im Web vor der Preisgabe identifizierender und persönlicher Informationen schützt. Die Erweiterung fasst Funktionen existierender Erweiterungen wie *Adblock* oder *NoScript* zusammen, die eine Preisgabe an Dritte zu unterbinden versuchen. Zusätzlich bietet NoTrace den Nutzern einen Einblick, welche Informationen beim Nutzen von Webdiensten an welche Anbieter preisgegeben werden und schafft somit Bewusstsein. Das Bewusstsein über ungewollte Informationsflüsse soll die Nutzer dabei unterstützen, fundierte Entscheidungen über die Verwendung der Webangebote und der Schutzmaßnahmen zu fällen.

Wills und Zeljkovic [152] präsentierten einen Ansatz, der die Preisgabe nicht verhindert, sondern die Nutzer vorerst über das Problem der Preisgabe informiert. Sie verfolgten das Ziel, die Nutzer in Bezug auf die Problematik personalisierter Werbung zu bilden. Um das Installieren von Software zu vermeiden, realisierten sie ihren Ansatz in Form einer zu besuchenden Webseite. Diese analysiert beim Besuch den Webbrowser-Verlauf des Nutzers über JavaScript, gleicht die besuchten Webseiten mit bekannten Webseiten ab, um involvierte Drittanbieter zu erfassen, und zeigt dem Besucher die gesammelten Informationen an. Zusammen mit einer Schätzung des Alters und des Aufenthaltsortes des Besuchers ermöglicht die Webseite so einen Einblick, wie weitreichend die Preisgabe von Informationen sein kann.

3.1.1.1 Soziale Onlinenetzwerke

Die Nutzer Sozialer Onlinenetzwerke sind sowohl Ziel als auch Quelle von Bedrohungen der Privatsphäre. Aufgrund der Masse an Nutzern und der Menge an geteilten persönlichen Informationen waren diese Webdienste häufig im Fokus der Forschung.

Aufbauend auf der zuvor beschriebenen Übertragung rechtlicher und sozialer Regeln auf Web-Systeme präsentierten Kang und Kagel [115] einen Ansatz für den Schutz der Privatsphäre: *Respect My Privacy* ermöglichte Nutzern von Facebook, OpenSocial und Friend-of-a-Friend ihre Profilinformationen mit einem Siegel zu versehen das bestimmt, wie Andere mit ihren Informationen umzugehen haben. Die Festlegung, dass andere Nutzer die Informationen beispielsweise nicht kommerziell nutzen dürfen, basierte dabei rein auf Vertrauen. Solche Siegel können die Nutzer dazu bringen, sich über die Verwendung der Daten Anderer Gedanken zu machen. Eine ähnliche Facebook-App präsentierte auch die Creative Commons [39].

Mahmood und Desmedt [124] betonen, dass der Fluss persönlicher Informationen verstärkt visualisiert werden müsse, um ihn für Nutzer verständlich zu machen. Dies soll den Nutzern erleichtern zu verhindern, dass Informationen ungewollt oder unerwartet in die Hände Anderer gelangen. In ihrer Arbeit präsentieren die Autoren Beispiele, wie Informationsflüsse im Kontext von Facebook visualisiert werden könnten und wie eine interaktive Kontrolle des Flusses integriert werden könnte.

Verschiedene Facebook-Apps widmen sich der Schaffung von Bewusstsein über Informationen, die ein Nutzer selbst mit seinen Freunden und dem Dienst teilt. Die *Privacy Awareness App* [16] zeigt Facebook-Nutzern auf eine recht einfache Weise, welche Daten sie mit dem Sozialen Onlinenetzwerk teilen, die zudem auch mit Apps geteilt werden können. Nach dem Erhalt einer Vielzahl notwendiger Berechtigungen sammelt die App über die Facebook-API einen Großteil der Information ihres Nutzers. Sie zeigt dem Nutzer alle diese Informationen in einer Übersicht an und ermöglicht ihm auch diese vollständig herunterzuladen.

Während sich viele Nutzer bewusst sind, welche Statusnachrichten oder Fotos sie kürzlich mit wem in ihrem Sozialen Onlinenetzwerk teilten, geraten alte Inhalte in Vergessenheit. Zudem ändern sich Freundeslisten mit der Zeit und damit auch, wer auf geteilte Inhalte Zugriff hat. In Form eines Spiels ermöglicht die App *Friend Inspector* [83] Nutzern, ihr Wissen über die Zugriffsrechte ihrer Freunde auf ihre Inhalte zu testen. In einer Personalisierungsphase werden Inhalte bestimmt, die in den Augen eines Nutzern besonders privat sind. Daraufhin muss der Nutzer unter Zeitdruck für Fotos oder Statusmeldungen bestimmen, welche Nutzer aus einer Menge angezeigter Profilbilder diese sehen können. Mit einer persönlichen Highscore und Vorschlägen zur Optimierung der Privatsphäre-Einstellungen endet das Spiel.

Die Diskrepanz zwischen dem Wissen um den Zugriffsschutz eigener Bilder und der realen Umsetzung dokumentierten Liu et al. [123] in einer Nutzerstudie. Anhand von Beispielbildern aus den Facebook-Fotos ihrer Studienteilnehmer erfassten sie, inwieweit das für ein Bild erwartete Publikum mit dem tatsächlichen übereinstimmte. Die Studie zeigte, dass bei nur 37 % der betrachteten Inhalte eine Übereinstimmung der Vorstellung und der Realität vorlag. Bei mehr als der Hälfte der Bilder waren sich die Nutzer nicht über das tatsächliche Publikum bewusst.

Das von Pötzsch beschriebene Privatsphäre-Paradoxon betrachteten Acquisti und Gross [70] am Fall von *The Facebook* im Jahr 2005, zu Zeiten, als das Soziale Onlinenetzwerk noch auf amerikanische Studierende beschränkt war. Sie zeigten, dass auch solche Personen, die ihre Privatsphäre schätzten, ihre persönlichen Daten teils äußerst großzügig preisgaben. Besonders zu beachten ist jedoch, dass ein Vergleich mit ihrer nur wenige Monate alten Vorstudie zeigte, dass sich das Teil-Verhalten der Nutzer durch aktuelle aufklärende Pressemeldungen verändert hatte und zu einer merklichen Einschränkung der preisgegebenen Information geführt hatte. Dies zeigt, dass Nutzer nach einer entsprechenden Aufklärung handeln und somit die Schaffung von Bewusstsein nicht nur ein notwendiges Kriterium ist, sondern auch förderlich für den Schutz der Privatsphäre.

Tuunainen et al. [143] untersuchten das Bewusstsein der Nutzer darüber, dass Andere auf ihre Profilinformationen zugreifen können. Während ihren Studienteilnehmern bewusst war, dass ihre Online-Profile ohne eigene Einschränkungen öffentlich sichtbar waren, war über der Hälfte der Teilnehmer nicht bewusst, dass Apps, die diese nutzen, auch auf ihre Daten zugreifen können und dass Facebooks Datenschutzvereinbarung erlaubte, ihre Daten für Werbezwecke weiterzuverwenden.

Um die bisher hauptsächlich auf Zugriffsschutz beruhenden Maßnahmen zum Schutz der Privatsphäre für die Nutzer verständlicher darzustellen und so beispielsweise die Reichweite der Freigabe von Informationen (das Publikum) deutlicher zu kommunizieren, setzen Soziale Onlinenetzwerke heute vermehrt auf Piktogramme. Ianella und Finden [112] untersuchten die Verwendung verschiedener Piktogramme als Ersatz für beschreibende Texte, um das Publikum geteilter Inhalte deutlich und knapp darzustellen. Sie weisen darauf hin, dass Piktogramme onlinenetzwerkübergreifend einheitlich sein sollten, um die Nutzer nicht zu wirren, da diese häufig gleichzeitig verschiedenen Netzwerken angehören. Holtz et al. [109] untersuchen Piktogramme für die Vermittlung verschiedener Informationen, wie beispielsweise die Preisgabe von Informationen, das Publikum geteilter Informationen und die Verwendung geteilter Informationen. Neben der Vereinheitlichung von Piktogramm-Sätzen betrachteten die Autoren das Verständnis von Piktogrammen über verschiedene Kulturen hinweg.

3.1.1.2 Weitere Anwendungsbereiche

Könings et al. [118] betrachteten Privacy Awareness im Kontext von Ubiquitous-Computing-Systemen, die Menschen in alltäglichen Situationen unterstützen und durch vielfältige Sensoren Informationen sammeln, deren unkontrollierte Preisgabe der Privatsphäre der Nutzer schaden kann. Am Beispiel eines Systems zur Herzfrequenzüberwachung präsentieren die Autoren ein Modell zur Modellierung von betroffenen Informationen und beteiligter Entitäten. Dies soll ermöglichen, gewollte und ungewollte Informationsflüsse zu untersuchen. Es bietet damit die Grundlage, um im Weiteren Nutzerschnittstellen zu schaffen, die über gesammelte Informationen und Empfänger informieren.

Iachello und Hong [111] liefern mit ihrer umfassenden Übersichtsarbeit aus dem Jahr 2007 einen Überblick vieler älterer Arbeiten aus dem Bereich der Privatsphäre und Mensch-Maschine-Interaktion verschiedener Anwendungsbereiche. Diese greifen zum Teil auch den Aspekt des Bewusstseins über die Preisgabe auf.

Allgemein lässt sich feststellen, dass die meisten Arbeiten bisher im Kontext des World Wide Webs entstanden sind. Jüngste Arbeiten wie die von Könings et al. zeigen jedoch, dass die Bewusstseinsschaffung im Kontext der Privatsphäre auch in anderen Anwendungsbereichen in den Fokus gerät.

3.1.2 IT-Sicherheit

Auch im Bereich der IT-Sicherheit wurden Techniken umgesetzt und evaluiert, die Bewusstsein schaffen sollen. Diese reichen vom grünen Vorhängeschlosssymbol in der URL-Leiste oder Statusleiste im Webbrowser, welches eine sichere Verbindung anzeigt, über Warnmeldungen zum Schutz vor Phishing-Angriffen bis hin zu visuellen Indikatoren für die Güte neu erstellter Passwörter. Im Folgenden werden ausgewählte Publikationen vorgestellt, auf die in dieser Dissertation Bezug genommen wird.

Whitten [150] widmete sich in ihrer Dissertation der Nutzbarkeit von IT-Sicherheit im Allgemeinen und untersuchte diese am Beispiel von E-Mail-Verschlüsselung. In ihrer Arbeit beschreibt sie verschiedene Eigenschaften, die die Nutzbarkeit von IT-Sicherheit häufig erschweren. Insbesondere die von ihr formulierte *secondary goal property* spielt auch beim Schutz der Privatsphäre eine entscheidende Rolle: Der Schutz von IT-Sicherheit respektive der Privatsphäre ist meist nicht das eigentliche Ziel der Nutzer und bekommt daher häufig nur wenig Beachtung.

Schechter et al. [132] untersuchten das Verhalten von Online-Banking-Nutzern während sie eingeblendete Hinweise und Warnungen des Webbrowsers manipulierten. Keiner ihrer Teilnehmer bemerkte das Fehlen einer HTTPS-Adresse oder des Schlosssymbols. Beim Ersetzen einer visuellen Anti-Phishing-Funktion durch eine Wartungsmeldung gaben 97 % von ihnen weiterhin ihre Login-Daten ein. Als zusätzlich auch eine fingierte Zertifikatswarnmeldung eingeblendet wurde, die davon

abriet fortzufahren, gaben immer noch 53 % der Teilnehmer ihre Daten ein. Dhamija et al. [88] untersuchten, an welchen Merkmalen Nutzer Phishing-Webseiten erkennen. 23 % ihrer Teilnehmern entschieden allein auf Basis der Merkmale des Webseiteninhalts. Weitere 36 % bezogen die URL der besuchten Webseite ein, betrachteten jedoch keine SSL-Indikatoren. Weitere 9 % achteten auf das „HTTPS“ in der URL-Leiste. Die übrigen 32 % achteten auch auf das Schlosssymbol. In ihrer Studie schenkten somit weniger als die Hälfte der Teilnehmer den Indikatoren des Webbrowsers Aufmerksamkeit als sie die Aufgabe hatten, legitime von betrügerischen Seiten zu unterscheiden. Beide Publikationen zeigen, wie wenig Beachtung Indikatoren und Hinweismeldungen von den Nutzern bekommen haben. Die Herausforderung an das Design effektiverer Indikatoren und die Notwendigkeit von Aufklärung werden deutlich.

Egelman et al. [90] verglichen aktive und passive Phishing-Warnmeldungen von Webbrowsern. Zwischen die Verkaufsbestätigungen realer Online-Einkäufe mischten sie fingierte E-Mails. 97 % ihrer Teilnehmer öffneten mindestens eine der in diesen E-Mails verlinkten Phishing-Webseiten. 90 % ihrer Kontrollgruppe ohne Warnmeldungen fielen auf das Phishing herein. Keiner der Nutzer des Webbrowsers Firefox mit aktiver Warnmeldung fiel dem Phishing zum Opfer. Hingegen fielen 45 % der Nutzer des Internet Explorers mit aktiver Warnung darauf herein und 90 % der Nutzer des Internet Explorers mit passiver Warnmeldung gaben ihre Daten preis. Die Ergebnisse zeigten die geringere Effektivität passiver Warnmeldungen.

Maurer et al. [127] erarbeiteten einen Ansatz der Sicherheitswarnmeldungen im Kontext einer Webseite anzeigt, ohne die Nutzer bei ihren Aktionen zu unterbrechen. Ihr Ansatz soll dem unbedachten Schließen aktiver Hinweismeldungen und dem Übersehen und Missachten passiver Indikatoren begegnen. Ziel des Ansatzes ist, die Aufmerksamkeit der Nutzer genau in dem Moment zu erhöhen, wenn diese kritischen Daten wie Kreditkartennummern oder Passwörter auf einer potenziell betrügerischen Webseite eingeben. Geben Nutzer kritische Daten auf einer nicht vertrauten Seite ein, so wird beim Tippen der Information eine Warnmeldung direkt neben dem Eingabefeld eingeblendet. Der Nutzer kann die Eingabe ungestört beenden. Das Verlassen des Feldes oder das Abschicken des Formulars wird jedoch verhindert, solange die Warnung nicht beachtet wurde. Durch den Aufbau einer persönlichen Whitelist wird die Zahl von Meldungen über die Zeit verringert. Eingaben auf vertrauten Webseiten werden durch unauffällige grüne Umrandungen verdeutlicht. Studienergebnisse der Autoren zeigen, dass die Darstellung der Warnungen im Kontext der aktuellen Nutzerinteraktion und damit im Fokus des Nutzers einen vielversprechenden Ansatz darstellt. In den Studien konnten so mehr betrügerische Webseiten von den Nutzern erkannt werden.

Shin und Lopes [134] untersuchten die Effektivität verschiedener visueller Indika-

toren, die Webnutzer vor einem SSL-Stripping-Angriff schützen sollen. Die Autoren präsentierten *SSLight*, das in Login-Formular-Feldern eines von drei Ampellichtern (rot, gelb, grün) einblendet, je nachdem ob die Formulardaten über eine sichere Verbindung übermittelt werden oder nicht. Alternativ präsentierten sie die Möglichkeit, die Hintergrundfarbe der Eingabefelder im Fall einer unsicheren Verbindung rot zu färben. In ihrer Studie verglichen sie beide Methoden mit der klassischen Textmeldung innerhalb eines Pop-up-Fensters, das beim Abschicken des Formulars über eine unsichere Verbindung erscheint. Beim Erscheinen des Pop-up-Dialogs fuhren 96 % der Teilnehmer mit der gestellten Aufgabe fort. Im Fall der Ampellichter schickten 64 % der Teilnehmer ein unsicheres Formular ab und im Fall der farblichen Hinterlegung sendeten nur 32 % das Formular über die unsichere Verbindung ab. Ihre Ergebnisse lassen darauf schließen, dass die präsentierten visuellen Indikatoren effektiver als die Pop-up-Meldung sind.

Ur et al. [144] präsentierten einen umfassenden Vergleich visueller Indikatoren zur Güte von Passwörtern. Die Teilnehmer ihrer Studie erstellten Passwörter mit der Unterstützung von 15 verschiedenen Indikatoren. Die Indikatoren hatten einen messbaren Einfluss auf die erstellen Passwörter. Passwörter, die mit der Unterstützung eines der 13 nicht rein textuellen Indikatoren erstellten wurden, waren statistisch signifikant länger. Am effektivsten waren Indikatoren, die Text und visuelle Darstellung vereinten. Das Aussehen der visuellen Darstellung schien keinen merklichen Einfluss zu haben.

3.2 Bilder und Metadaten

Verschiedene Arbeiten untersuchten Herausforderungen, die durch geteilte Bilder entstehen. Im Folgenden werden einige ausgewählte Arbeiten vorgestellt.

3.2.1 Quelle der Bedrohungen

Ahern et al. [71] untersuchten Faktoren von Privatsphäre-Entscheidungen, die bestimmen, ob Fotos öffentlich oder nur einschränkt sichtbar geteilt werden und damit, ob eine Bedrohung durch Andere wahrgenommen wird. Die Autoren analysierten geteilte Fotos, Tags und Privatsphäre-Einstellungen von Bildern, die ihre Studienteilnehmer über Mobiltelefone bei Flickr geteilt hatten. Die Ergebnisse zeigten, dass der Ort eines Fotos häufig die Privatsphäre-Einstellung (öffentlich sichtbar oder nicht) beeinflusste. Trotzdem wurde bei nur 2 % der Fotos die funkzellenbasierte Angabe des Aufnahmeortes unterdrückt. Fotos mit personenbezogenen Tags wie Namen waren signifikant häufiger privat als Fotos mit textuellen Beschreibungen zu Orten, Aktivitäten oder Veranstaltungen. In Interviews identifizierten Ahern et al. vier Variablen der Abwägung des Teilens: Sicherheit betroffener Personen und deren Hab

und Guts, Pflege der Online-Identität, Preisgabe gegenüber bekannten Personen und die gewollte Zugänglichkeit für Andere. Teilnehmer mit Familie und Kindern waren generell mehr über die Privatsphäre von Bildern besorgt. Hier spielte auch die Angabe des Aufnahmeortes häufiger eine Rolle. Die Teilnehmer fühlten sich teilweise gezwungen Bilder öffentlich zu teilen, damit alle ihre Bekannten die Bilder auch sehen können, ohne einem Dienst erst beitreten zu müssen.

Strater und Lipford [138] untersuchten in Interviews das Teil-Verhalten, getätigte Zugriffsbeschränkungen und die zugrunde liegende Motivation von Studierenden im Sozialen Onlinenetzwerk Facebook. Sie stellten fest, dass ihre Teilnehmer viele Informationen und Privatsphäre-Einstellungen einmalig beim Beitreten zum Sozialen Onlinenetzwerk tätigten, sie später zwar erweiterten, jedoch selten vorhandene Informationen überprüften. Dies führte dazu, dass viele Teilnehmer nicht wussten, was sie selbst preisgaben oder was ihre eigenen Privatsphäre-Einstellungen waren. Die Teilnehmer sahen am häufigsten eine Bedrohung ihrer Privatsphäre durch Stalker oder Fremde, die sie ausfindig machen könnten. Reale Negativerlebnisse dieser Art waren der häufigste Auslöser, ihre geteilten Informationen zu überarbeiten. Die Autoren stellten fest, dass das wahrgenommene Publikum geteilter Informationen zu schrumpfen schien, wenn die Teilnehmer verstärkt mit ausgewählten Personen aus ihrem sozialen Netzwerk kommunizierten und ihnen so das wahre Publikum nicht mehr bewusst war. Das Betrachten anderer teils öffentlicher Profile bewegte die Teilnehmer dazu, ihre eigenen geteilten Profilinformationen infrage zu stellen. Im Fall geteilter Fotos war dieses überraschenderweise nicht zu beobachten.

Mittels Fokusgruppen untersuchten Besmer und Lipford [77] die Wahrnehmung von Privatsphäre im Kontext Sozialer Onlinenetzwerke, die das Teilen von Fotos und das Markieren von Personen auf Fotos ermöglichen. Ihre Teilnehmer hatten in den meisten Fällen ein klares Bild, wer ihre Privatsphäre bedrohen könnte. Die Teilnehmer sahen Personen aus ihrem Bekanntenkreis als Bedrohungsquelle an, allen voran die Mitglieder ihrer Familie. Keiner von ihnen sah hingegen Fremde als Quelle der Bedrohung. Der hauptsächliche Grund ihrer Bedenken war der Wunsch nach positivem Erscheinen innerhalb ihres Online-Bekanntschaftskreises.

Johnson et al. [113] untersuchten in einer Studie die Privatsphäre-Sorgen von Facebook-Nutzern sowie die von diesen verfolgten Schutzstrategien. Ihre Studie zeigte, dass 84,6 % ihrer Teilnehmer den Zugriff auf ihre Profile eingeschränkt hatten und somit ihrer größten Sorge, dem Zugriff durch Fremde, durch die allgemeinen Privatsphäre-Einstellungen effektiv begegneten. Die Autoren stellten bei ihren Teilnehmern eine verstärkt empfundene Bedrohung durch bestimmte Mitglieder ihrer Freundesliste fest, wie Familienmitglieder oder Kollegen im Beruf. 37 % ihrer Teilnehmer wollten nicht, dass bestimmte Freunde ihr Profil oder bestimmte Beiträge zu sehen bekommen. Die Autoren stellten fest, dass nutzerdefinierte Listen zur Gruppierung von Freunden in diesem Fall nicht helfen, da diese meist im Vorfeld erstellt

werden und im Fall des Teilens die Schutzbedürfnisse für einzelne Beiträge oder Fotos nicht abdecken können. Bisherige Mechanismen zur Zugriffskontrolle erweisen sich laut den Autoren als nicht ausreichend. Auf Basis ihrer Ergebnisse differenzierten Johnson et al. die Quelle der Bedrohung in weitere Untergruppen von Fremden und Freunden, wie Personen, die ein Nutzer nicht persönlich kennt, oder Berufskollegen.

3.2.2 Bedrohungen durch Bild-Metadaten

Während die vorherigen Studien neben einer Bedrohung durch Profilinformationen vorwiegend die Markierungen von Personen auf Fotos kritisch betrachteten, widmeten sich Friedland und Sommer [96] der Evaluierung der häufig genannten Bedrohung durch Ortsangaben innerhalb von Fotos. Mit ihrer Arbeit zeigten sie exemplarisch, wie diese Informationen Schlüsse auf reale Orte erlauben. Auf Basis von öffentlichen Kartendiensten und ortsbasierten Suchfunktionen verschiedener Webdienste zeigten sie, wie der wahrscheinliche Wohnort anonymer Online-Verkäufer sowie der von YouTube-Nutzern ausfindig gemacht werden konnte. Außerdem zeigten sie wie ein privater Twitter-Account einer Person des öffentlichen Lebens auf Basis von Ortsinformationen identifiziert werden konnte. Die Autoren weisen auf die Vorzüge von Metadaten hin. Sie fordern einen besseren Schutz durch eine Entlastung der Nutzer durch eine Vereinheitlichung von Privatsphäre-Strategien (Opt-out, nicht global). Zudem sollen entsprechende Technologien die Nutzer schützen, indem beispielsweise Nachkommastellen von Koordinaten entsprechend Nutzerwünschen gekappt werden.

3.2.3 Klassifizierung der Privatheit von Bildern

Zerr et al. [155] präsentierten Methoden zur automatischen Erkennung privater Bilder auf Basis von maschinellem Lernen. Auf Basis von Bildern des Dienstes Flickr, den zugehörigen Bild-Metadaten und einer manuell durchgeführten crowdsourcingbasierten Klassifizierung der Bilder in privat oder öffentlich trainierten und evaluierten sie Modelle für die Klassifizierung von Bildern. Die Klassifizierung erlaubt, einen Datenbestand nach vermeintlich privaten Bildern zu durchsuchen oder Suchergebnisse nach der klassifizierten Privatheit der Motive zu diversifizieren und zu ordnen. Aufbauend auf der Klassifizierung präsentierten Zerr et al. *PicAlert!* [154], einen Demonstrator für die Klassifizierung der Suchergebnisse einer Schlagwortsuche beim Fotodienst Flickr und für die Klassifizierung eigener Bilder. Die Klassifizierung der Privatheit eines Bildes kann einen Nutzer unterstützen, passende Privatsphäre-Einstellungen beim Teilen des Bildes zu wählen. Sie kann auch verwendet werden, um Bildbestände zu filtern oder zu sortieren, die durch die in dieser Dissertation präsentierten Methoden zur Schaffung von Bewusstsein über relevante Bilder gefunden werden. So kann der Umgang mit großen Mengen von Bildern verbessert werden, indem sich die Nutzer zuerst mit potenziell privaten Bildern befassen können.

3.2.4 Bewusstsein über Bilder anderer Nutzer

Burghardt et al. [82] präsentierten einen Ansatz zur Schaffung von Bewusstsein über Fotos, die Andere innerhalb von Web-2.0-Diensten teilen, welche die Privatsphäre einer abgebildeten Person betreffen könnten. *Privacy for Image Objects* (PRIMO) hat zum Ziel, Nutzer über Fotos zu informieren oder sogar das Teilen von Bildern zu verhindern, wenn eine entsprechende nutzerdefinierte Regel auf sie zutrifft. Auf das Verhindern der Veröffentlichung von Bildern gehen die Autoren nicht weiter ein. Für das Erfassen von Bildern verbindet sich der Mash-up-Dienst mit Sozialen Onlinenetzwerken oder anderen Diensten zum Teilen von Fotos und indexiert deren Fotos unter der Verwendung von Gesichtserkennung sowie einer grundlegenden Klassifizierung abgebildeter Personen, wie beispielsweise der Bestimmung ihres Geschlechts. Nutzer spezifizieren persönliche Regeln wie „informiere mich über Bilder von mir mit Personen, die ich nicht kenne“. Personen, die ein Nutzer kennt, können durch den Import von Kontaktlisten der verschiedenen Dienste festgelegt werden. Nach der Definition einer Regel oder nach dem Hochladen neuer Bilder werden die definierten Regeln ausgewertet und die festgelegten Aktionen ausgeführt. Die Autoren betrachten nicht, wie die Nutzer der Bereitstellung von Trainingsbildern ihrer selbst für die Gesichtserkennung gegenüberstehen. Auf die Erkennung von Freunden und die dazu notwendigen Trainingsbilder gehen sie nicht weiter ein. Die heutige Masse an geteilten Bildern und die darauf abgebildete Vielzahl von Menschen lassen vermuten, dass das beschriebene System wohl nicht allgemein, sondern nur auf Fotos von Online-Freunden beschränkt skaliert, da keine Vorauswahl zu prüfender Bilder getroffen wird. Burghardt et al. lassen viele Aspekte in ihrer Beschreibung aus, wie beispielsweise auch wessen Fotos wann analysiert und berücksichtigt werden oder wie das Hochladen neuer Fotos registriert wird. Die Publikation lässt viele Fragen offen. Die präsentierte regelgesteuerte Benachrichtigung könnte die in dieser Dissertation beschriebenen Ansätze ergänzen.

3.2.5 Kontrolle über Bilder anderer Nutzer

Kann Bewusstsein über geteilte Bilder geschaffen werden, müssen Nutzer die Möglichkeit haben, Kontrolle über potenziell bedrohliche Inhalte auszuüben.

Aufbauend auf ihren vorherigen Arbeiten präsentierten Besmer und Lipford [78] *Restrict Others*, das Facebook-Nutzer unterstützen soll, Fotobesitzer zur Einschränkung von Zugriffsrechten bestimmter Fotos zu veranlassen. Restrict Others erlaubt einem Nutzer eine Anfrage an den Besitzer eines Bildes zu stellen, dass bestimmte Personen vom Zugriff auf ein Bild ausgeschlossen werden, auf dem er markiert wurde. Die Facebook-App formalisiert auf diese Weise die notwendige Kommunikation zwischen den Beteiligten, die sonst häufig über persönliche Nachrichten abläuft, und integriert sie in das Bilder-Management. Sie unterstützt die Nutzer beim Schutz ihrer

Privatsphäre, indem sie hilft, Wünsche zur Kontrolle von Bildern Anderer zu kommunizieren. Um Nutzer zuvor auf die entsprechenden Fotos aufmerksam zu machen, baut die App auf die vorhandenen Benachrichtigungen über neue Markierungen durch Facebook. Bei einer Evaluierung durch eine Laborstudie waren nur zwei von 17 Teilnehmern gegen das vorgestellte Konzept. Einige Teilnehmer wünschten sich, ohne Interaktion direkt die Rechte von Bildern ändern zu können.

Squicciarini et al. [136] präsentierten mit *Collaborative Privacy Management* einen Ansatz zum gemeinschaftlichen Besitz von Fotos und der gemeinsamen Bestimmung von Zugriffsrechten. CoPE ermöglicht allen Betroffenen eines Bildes, an der Bestimmung der Zugriffsrechte für das Bild teilzuhaben. Durch das Markieren von Personen auf einem Bild werden diese zu Betroffenen und können daraufhin den Ko-Besitz beantragen. Jeder Ko-Besitzer eines Bildes kann seine bevorzugten Zugriffsrechte für ein Bild festlegen. Das Publikum (nur Ko-Besitzer, öffentlich, einige Freunde) wird anschließend durch Mehrheitsbestimmung ermittelt und die Zugriffsrechte werden dementsprechend festgelegt, wobei im Fall „einiger Freunde“ die Schnittmenge von Personen aller Einzelfestlegungen verwendet wird. Der als Facebook-App realisierte Prototyp zum kollaborativen Privatsphäre-Management wurde im Rahmen einer Studie von den meisten Teilnehmern positiv bewertet.

In einer qualitativen Studie auf Basis von Interviews und Fokusgruppen erfassten Lampinen et al. [121] Strategien von Nutzern Sozialer Onlinenetzwerke, die dem Schutz der eigenen Privatsphäre dienen, wenn andere Nutzer Informationen über sie preisgeben. Ihre Sammlung präventiver und korrigierender Maßnahmen soll als Basis für das Design neuer technischer Methoden dienen. Als eine besondere Herausforderung beschreiben sie die Schaffung einer kollaborativen, präventiven Lösung, die Nutzern ermöglichen soll, ihre Anforderungen zur Wahrung der Privatsphäre vor dem Entstehen von Problemen abzugleichen. Auf diese Weise könnten Inhalte vollständig geschützt werden, während korrigierende Maßnahmen wie *Restrict Others* nicht verhindern können, dass jemand ein Bild sieht, bevor der Zugriff beschränkt wird. Als einen möglichen Ansatz schlagen Lampinen et al. einen Vorschaubereich innerhalb Sozialer Onlinenetzwerke vor, in dem betroffene Personen unter sich einen Konsens zur Veröffentlichung von Inhalten wie Fotos finden können, bevor sie mit dem vollständigen Publikum geteilt werden.

3.2.6 Kontrolle über eigene Bilder

Um das voreilige und unüberlegte Teilen von Bildern zu minimieren, schlugen Ahern et al. [71] einen Ansatz vor, der dem von Lampinen et al. ähnelt. Sie regten an, eine Art Wartebereich beim Teilen von Fotos zu etablieren, in dem Bilder vorerst verweilen, bis sie nochmals explizit für das Teilen mit Anderen freigegeben wurden. In ihrer Studie hatten die Nutzer im Nachhinein die Privatsphäre-Einstellungen von 7 % der

Fotos (35 % auf eingeschränkt, 65 % auf öffentlich) geändert. Der vorgeschlagene Wartebereich könnte dafür sorgen, dass solche Bilder nicht in falsche Hände geraten und dass Bedrohungen für die Nutzer selbst und für Andere verringert werden.

Verwendung von Metadaten Klemperer et al. [117] untersuchten, inwieweit Tags wie Schlagworte und Bildtitel verwendet werden können, um intuitive Zugriffsschutzregeln für Fotos zu erstellen. In einer Laborstudie zeigten sie, dass Tags, die für die Organisation von Bildern vergeben wurden, schon für annehmbar gute Ergebnisse bei der Erstellung von Zugriffsschutzregeln verwendet werden konnten. Die Autoren zeigten weiter, dass die Teilnehmer mit dem Wissen über den Einsatz eines tagbasierten Zugriffskontrollsystems mit nur leichten Veränderungen ihrer Tags schon deutlich effektivere Ergebnisse erzielen konnten. Durch eine Modifikation ihrer Tags mit dem Wissen um ihre persönlichen generierten Regeln wurde die Effektivität noch weiter verbessert. Mit ihrer Arbeit zeigen die Autoren, wie Bild-Metadaten verwendet werden können, um den Zugriff auf eigene Bilder effektiv einzuschränken, und so die Privatsphäre zu schützen.

Schutz vor ungewollter Weitergabe Die Facebook-App *McAfee Social Protection* [29] verspricht seinen Nutzern, dass Andere ihre Bilder nicht vervielfältigen oder weiterzugeben können. Um die App zu nutzen, müssen sowohl die Teilenden als auch die autorisierten Betrachter die Facebook-App und eine Webbrowser-Erweiterung verwenden, die nur für das Betriebssystem Windows 7 und die Browser Firefox und Internet Explorer existiert. Nicht autorisierte Nutzer und Nutzer anderer Browser sehen nur eine verschwommene Version eines Bildes, da sie keinen Zugriff auf das bei McAfee gespeicherte Original bekommen. Die Browser-Erweiterung soll das Kopieren in die Zwischenablage verhindern. Sie kann jedoch letztendlich nur Laien eine Vervielfältigung erschweren. Der Erfolg dieses Ansatzes ist ebenso kritisch zusehen wie der ausbleibende Erfolg des Fehlansatzes *X-pire!* [50], welcher versprach, dass das Internet Bilder „vergessen“ kann. Bilder, denen durch X-pire! und die dazugehörige Webbrowser-Erweiterung ein „digitales Verfallsdatum“ verpasst werden sollte, wurden beim Teilen verschlüsselt. Für das Betrachten mussten die Nutzer die Erweiterung zum Entschlüsseln installiert haben. Widerrief ein Bildbesitzer den Schlüssel für ein Bild, so sollte es von diesem Zeitpunkt an nicht wieder entschlüsselt werden können. Verschiedene konzeptionelle Schwächen waren das Aus für den Ansatz.

3.3 Standortinformationen

Die Privatheit von Ortsinformationen und die Bedrohung der Privatsphäre durch Standortangaben ist schon seit über 10 Jahren Thema der Forschung.

Krumm [119] stellte zeitnah nach dem Erscheinen des ersten iPhones eine Übersicht bisheriger Arbeiten zu Ortsinformationen und Privatsphäre zusammen. Diese umfasst Bedrohungen, Schutzmaßnahmen und die Wahrnehmung von Nutzern. Viele der vorgestellten Arbeiten beziehen sich auf Anwendungsgebiete wie die Verkehrsüberwachung oder die Nutzung von GPS-Trackern. Sie haben meist nur einen theoretischen Bezug zu den heute verbreiteten hier betrachteten Diensten.

Krumm trägt in seiner Arbeit Ergebnisse von Nutzerstudien aus den Jahren 2001 bis 2007 zusammen, deren nahezu einheitliches Ergebnis war, dass sich die Nutzer kaum um die Preisgabe von Ortsinformationen sorgten. Die Nutzer waren bereit, Bewegungsprofile von Wochen bis zu einem Monat und teils mehr gegen einen eher geringen monetären Ausgleich mit jemandem zu teilen. Der Preis variierte abhängig davon mit wem die Information geteilt würden. Einige Teilnehmer waren sogar bereit, ihre Daten für nur geringfügig höhere Entschädigungen auch für die kommerzielle Nutzung freizugeben. In den letzten Jahren hat sich mit der starken Verbreitung mobiler Geräte und der Mannigfaltigkeit der mobilen Apps auch die Nutzung von Standortinformationen deutlich erhöht. Dies hat auch Auswirkung auf die Empfindungen der Nutzer und ihr Schutzbedürfnis für die Ortsinformationen genommen, wie die in Abschnitt 3.3.3 und Kapitel 5 präsentierten Studien zeigen.

3.3.1 Schutz von Standortinformationen

In der Vergangenheit wurden diverse Maßnahmen veröffentlicht, die dem Schutz der Privatsphäre vor Bedrohungen durch Ortsinformationen dienen [119].

Um die wahre Identität von Nutzern zu schützen, können innerhalb von standortbezogenen Diensten Pseudonyme verwendet werden, um die Zuordnung von Standortinformationen zu Personen zu erschweren. Um Schlüsse auf die wahre Identität weiter zu erschweren, können solche Pseudonyme regelmäßig oder situativ bedingt gewechselt werden. Eine darüber hinaus häufig betrachtete Form von Anonymität ist die sogenannte k-Anonymität, bei der ein Nutzer nicht von $k-1$ anderen Nutzern unterschieden werden kann. Um dies für Ortsangaben zu erreichen, wird die Genauigkeit einer Angabe so weit verringert, dass die Ortsbeschreibung auf k Personen zutrifft: den Nutzer und $k-1$ nächste Personen. Wie Gruteser und Grunwald [99] beschreiben, kann bei dieser Anonymisierung zusätzlich die Genauigkeit der Zeit verringert werden, so dass nur bekannt ist, dass sich der Nutzer sowie $k-1$ Andere in einem bestimmten Zeitintervall in einem bestimmten Bereich befunden haben.

Eine weitere Möglichkeit den eigenen Standort bei der Verwendung von stand-

ortbezogenen Diensten zu schützen, ist die parallele Verwendung falscher Orte, wie sie Kido et al. [116] beschreiben: Eine Anfrage an einen standortbezogenen Dienst wird für mehrere Orte gleichzeitig gestellt und erst auf Nutzerseiten wird die korrekte Antwort aus allen Antworten gewählt. Diese Art von Schutz verursacht jedoch höhere Kosten in Form von Rechenzeit, Bandbreite oder Speicherplatz und ist somit nur bedingt einsetzbar. Zusätzlich ist es schwierig falsche Orte so zu wählen, dass sie von einem Angreifer nicht leicht als solche identifiziert werden können. Vonseiten der Dienstanbieter spricht gegen diese Schutzfunktion, dass durch gefälschte Daten die Funktion mancher standortbezogener Dienste beeinträchtigt wird.

Neben der k-Anonymität gibt es weitere Verfahren, die verwendete Koordinaten verändern und so den Standort eines Nutzers verschleiern. Ardagna et al. [72] präsentieren einen Ansatz der durch die geometrischen Operationen Verschieben, Radius vergrößern oder verkleinern eine Ortsangabe verändert. Der Radius entspricht dabei der Ungenauigkeit der Standortbestimmung, die durch die eingesetzte Technik entsteht. Werden Bewegungsprofile oder Sammlungen einzelner Standortangaben verwendet, können diese verschleiert werden, indem Rauschen zu den Daten hinzugefügt wird. Alternativ können die Ortsinformationen auf ein gröberes zeitliches und räumliches Raster abgebildet werden.

Ein großer Teil der Arbeiten zur Wahrung der Anonymität und der Verschleierung von Standortinformationen entstand vor den heutigen mobilen Geräten und standortbezogenen Diensten und Apps. Sie sind nur teilweise auf das heutige Dienstangebot zu übertragen. Da viele Apps und Dienste einzelne Standorte von Nutzern verarbeiten oder speichern, finden Methoden zum Schutz ganzer Bewegungsprofile nur beschränkt Anwendung. Aufseiten der Dienstanbieter können daraus Profile entstehen, doch aufseiten der Nutzer oder etwaiger Schutzdienste werden meist einzelne Informationen erfasst und weitergegeben.

Bei Verschleierungsmethoden die Flächen erzeugen, wie bei der Schaffung von k-Anonymität oder dem Einbeziehen und Vergrößern der Ungenauigkeit, ist zu beachten, dass viele der heutigen Dienste nur genaue Angaben von Zeit und Ort kennen. Die Angabe der Genauigkeit wird von vielen standortbezogenen Diensten gar nicht beachtet. Werden durch eine Schutzmaßnahme Flächen oder Zeiträume erzeugt, müssen diese für die Dienstnutzung meist auf einen Zeitpunkt und auf repräsentative Koordinaten reduziert werden.

3.3.2 Schutz von Standortinformationen unter Android

Im Rahmen von Entwicklungsprojekten wurden verschiedene Erweiterungen des quelloffenen Betriebssystems Android geschaffen, die die eingeschränkten Schutzmöglichkeiten für persönliche Informationen wie Standortinformationen verbessern. Darüber hinaus wurden auch im Rahmen der Forschung verschiedenen Anpassun-

gen des Betriebssystems vorgestellt, die sich der Analyse der Nutzung persönlicher Informationen und ihrem Schutz widmen.

3.3.2.1 Android-Erweiterungen in Entwicklungsprojekten

Die community-basierte Android-Distribution *CyanogenMod 7* [9] erweiterte Android 2.3 so, dass einer App nach ihrer Installation einzelne implizit gewährte Berechtigungen wieder entzogen werden konnten. Griff eine App, der die notwendigen Rechte entzogen wurden, auf den Aufenthaltsort zu, so erzeugte dies eine `Security Exception`. Da manche Apps gegen diese Reaktion nicht korrekt gewappnet waren, beendeten sie sich mit einem Fehler und waren nicht mehr funktionsfähig. Beim Wechsel auf die Code-Basis von Android 4 im Rahmen von CyanogenMod 9 wurde die Funktion nicht wieder integriert. Im Rahmen von CyanogenMod 10 wurde *Privacy Guard* eingeführt, das für einzelne Apps den Zugriff auf persönliche Informationen wie auch den Standort unterbinden kann. Durch eine Kombination aus Patch und einer App zur Rechteverwaltung ermöglicht *PDroid 2.0* [51] auf gerooteten Android-Systemen den Zugriff auf persönliche Daten zu unterbinden. Die Erweiterung ermöglicht zudem, gefälschte Informationen an Apps zu geben. So können im Fall von Ortsinformationen statt des wirklichen Ortes fixe oder zufällige Koordinaten an Apps gegeben werden. Auf einem Gerät mit Root-Zugriff ermöglicht die App *LBE Privacy Guard* das Blockieren von Zugriffen auf persönliche Informationen. Die App überwacht dazu App-Zugriffe auf die persönlichen Daten und fragt den Nutzer im Fall eines Zugriffs, ob er den Zugriff gewährt oder nicht. Alternativ kann der Zugriff auf Dauer blockiert oder erlaubt werden. Mit *App Ops* (zu deutsch: App-Vorgänge) brachte Android 4.3 von Haus aus eine versteckte Funktion mit, die Nutzern das Entziehen von Berechtigungen erlaubte. App Ops zeigte dem Nutzer zudem, wie häufig eine App Zugriff auf die Daten genommen hatte und wann der letzte Zugriff stattgefunden hatte. Mit dem Erscheinen von Android 4.4.2 wurde die Funktion jedoch wieder entfernt und ihre Zukunft ist ungewiss.

Aus Sicht der Nutzer ist der Schutz der Privatsphäre ein Argument für das Einschränken von Rechten oder die Manipulation preisgegebener Daten. Für App-Entwickler sprechen mindestens zwei Gründe dagegen: Apps könnten auf modifizierten Systemen nicht korrekt funktionieren oder aufgrund eines Fehlers beendet werden, wenn sie mit fehlenden Rechten und dadurch entstehenden Fehlern oder ausbleibenden Antworten nicht ausreichend umgehen. Besonders bei kostenfreien Apps kann das Beschränken von Berechtigungen zudem dafür sorgen, dass Werbung unterdrückt wird und somit das Geschäftsmodell von App-Anbietern untergraben wird. Dies mögen Gründe sein, die bisher einer dauerhaften Integration einer solchen Funktion entgegen gewirkt haben.

3.3.2.2 Android-Erweiterungen in der Forschung

TaintDroid [91] erweiterte Android 2.1 um dynamisches Taint-Tracking, welches erlaubt, persönliche Informationen programmatisch zu markieren und ihre Verwendung innerhalb einer App und ihre Weitergabe zwischen Apps zu verfolgen. Außerdem erlaubt es zu beobachten, wenn diese Informationen ein Gerät über das Netzwerk verlassen. Das Taint-Tracking ermöglicht zu prüfen, ob Apps persönliche Daten über den versprochenen Nutzen hinaus verwenden und ungewollt an Dritte preisgeben.

AppFence [110] erweiterte TaintDroid um zwei Schutzfunktionen für die Privatsphäre der Nutzer: Persönliche Daten können durch harmlose Platzhalter ersetzt werden. Außerdem ermöglicht es, eine durch das Taint-Tracking erkannte Preisgabe von Informationen über das Netz zu blockieren. Ortsinformationen können so auch geschützt werden. Sie werden durch die konstanten Koordinaten des Unternehmenssitzes von Google ersetzt. Anhand einer Stichprobe von 50 Apps zeigten die Autoren, dass 66 % der Apps ohne Nebenwirkungen durch AppFence geschützt werden konnten. Die übrigen 34 % benötigen die persönlichen Informationen um die gewünschten App-Funktionen bieten zu können.

MockDroid [76] ist eine modifizierte Version von Android 2.2, die Nutzern ermöglicht ihre Privatsphäre zu schützen, indem Anwendungen beim Zugriff auf geschützte Sensordaten oder persönliche Daten lediglich Platzhalterinformationen statt den echten Daten erhalten. Für jede App können die Nutzer für verschiedene Informationen bestimmen, ob auf echte oder gefälschte Daten zugegriffen wird. MockDroid implementiert diesen Schutz unter anderem auch für grobe und genaue Standortinformationen eines Gerätes. Stellt eine App eine Anfrage nach Ortsinformationen, wird ihr vorgegaukelt, dass keine Ortsinformationen vorliegen beziehungsweise bestimmt werden können.

MyShield [74] integriert grundlegende Techniken zur Anonymisierung von persönlichen Daten in Android 2.3. Die Autoren plädieren dafür, die Genauigkeit der preisgegebenen Informationen nicht an unverständliche Berechtigungen zu binden, sondern in Anlehnung an soziale Kreise an verschiedene Vertrauensniveaus. Durch die Umsetzung drei verschiedener Niveaus ermöglicht MyShield Nutzern zu entscheiden, ob sie einer App vollständig, teilweise oder gar nicht vertrauen und diese entsprechend unveränderte, anonymisierte oder gar keine persönlichen Daten erhält. Die Implementierung beinhaltet auch einen Schutz für Ortsinformationen. Bei vollem Vertrauen erhält eine App die genauen Ortsinformationen. Bei eingeschränktem Vertrauen werden die Koordinaten in Dezimalschreibweise nach der ersten Nachkommastelle abgeschnitten. Wird einer App misstraut, so erhält sie die fixen Null-Koordinaten N 0°, E 0°.

3.3.3 Studien zur Privatheit von Standortinformationen

Verschiedene Studien befassten sich mit Aspekten der Privatheit preisgegebener Standortinformationen.

3.3.3.1 Granularität preisgegebener Standortinformationen

Consolvo et al. [84] führten noch vor der Verbreitung mobiler Geräte, Sozialer Onlinenetzwerke und standortbezogener Webdienste eine Nutzerstudie über die Preisgabe von Ortsinformationen gegenüber sozialen Kontakten des realen Lebens durch. Mit Hilfe von PDAs erfassten sie durch Experience Sampling Informationen über den aktuellen Kontext von Nutzern zusammen mit ihrer Entscheidung, ob und mit welchem Detailgrad sie einer hypothetischen Anfrage einer bestimmten Person nach ihrem aktuellen Standort stattgeben würden oder diese verneinen würden. Bei 77 % der Anfragen waren die Teilnehmer bereit die Anfrage nach ihrem Ort zu beantworten. Dabei erlaubten sie in 77 % der Fälle genaue Ortsangaben (Adresse, Sehenswürdigkeit), bei 19 % der Anfragen grobe Ortsangaben (Stadt) und bei den übrigen nur vage Angaben (Bundesland, Land). Die Wahl des Detailgrads wurde dabei oft mit „am meisten für den Empfänger sinnvoll“ begründet und nicht mit Privatsphäre-Bedenken, welche meist die Nicht-Preisgabe begründeten. Als Faktoren der Entscheidung über die Preisgabe identifizierten die Autoren den Empfänger der Information (Lebenspartner, Arbeitskollegen, Freunde et cetera) sowie den möglichen/vermuteten Grund einer Anfrage. 56 % der Teilnehmer äußerten in nachgelagerten Interviews Bedenken gegenüber realen standortbezogenen Diensten.

Ahern et al. [71] untersuchten auch Aspekte der Privatheit von Ortsangaben beim Teilen von Bildern. Ihre Interviews zeigten, dass ihre Teilnehmer verschiedenen Granularitäten bei der Preisgabe von Ortsangaben zu Bildern als angemessen empfanden. Die meisten hatten keine Bedenken bei der Preisgabe der Stadt oder des Postleitzahlenbereichs, sie waren jedoch gegen das Verbreiten einer genauen Adresse.

Tang et al. [141] verglichen in einer Nutzerstudie zwei Möglichkeiten Regeln zum Teilen von Ortsinformationen zu definieren. Sie vergleichen den bis heute häufig in der Praxis verwendeten Ganz-oder-gar-nicht-Ansatz, der Nutzern erlaubt entweder keine Ortsangabe oder den genauen Ort zu teilen, mit der Möglichkeit aus vier verschiedenen Detailgraden abstrakter Ortsbeschreibungen, wie etwa der Adresse oder dem Namen der Stadt, zu wählen. Aus ihren Ergebnissen schlossen die Autoren, dass zusätzliche Detailgrade zu einem offeneren Teil-Verhalten führen können und die Nutzer eher ermuntern, häufiger ihren Standort mit anderen zu teilen. Gleichzeitig stellten sie fest, dass ihre Teilnehmer trotz der höheren Komplexität der Auswahl angaben, sich im Fall der größeren Auswahl wohler zu fühlen.

Die Ergebnisse der Studien sprechen für eine Bestimmung des Detailgrads geteilter Ortsinformationen aufseiten der Nutzer.

Zugriffskontrollmechanismen Benisch et al. [75] untersuchten, inwieweit komplexe Regeln zur Zugriffssteuerung die Privatsphäre-Bedürfnisse von Nutzern verbessert erfüllen können. In einer Nutzerstudie untersuchten sie auf Basis erfasster Bewegungsprofile, inwieweit unter anderem die generelle Freigabe bestimmter Orte oder die Freigabe von Daten bestimmter Wochentage/Tageszeiten die Wünsche der Teilnehmer abbilden können. Sie zeigten, dass die von ihnen betrachteten Regeltypen effektiver als Nutzer-Whitelists seien und in einigen Fällen eine Verbesserung der Abdeckung der Nutzerwünsche um den Faktor drei erreicht wurde. Schon in einer Vorstudie hatten die Teilnehmer angegeben, sich mit genauer formulierbaren Regeln wohler zu fühlen und folglich verstärkt ihren Standort preisgeben zu wollen. Benisch et al. streben an, zukünftig auch die Genauigkeit von preisgegeben Ortsangaben als weitere Dimension von Regeln zu untersuchen. Bei den präsentierten und geplanten Untersuchungen bleibt jedoch außen vor, dass die Nutzer meist ihren genauen Ort mit Dienstanbietern teilen. Somit verlassen die Informationen ihren Kontrollbereich und nur Zugriffskontrollen schränken ein, wer die persönlichen Informationen sehen darf. Eine Beschränkung der Genauigkeit der Ortsinformationen aufseiten der Nutzer wird nicht in Betracht gezogen.

Standortbezogene Dienste in der Praxis In den letzten Jahren entstanden über 100 Dienste, wie *Google Latitude* oder *Foursquare*, die Nutzern erlauben ihren aktuellen Standort mit anderen zu teilen. Nur wenige dieser Dienste erlauben ihren Nutzern bisher die Kontrolle über die Granularität der veröffentlichten Ortsangaben.

Tsai et al. [142] berichteten, dass lediglich 11 von 89 untersuchten Diensten dies ermöglichten. Beispielsweise Google Latitude erlaubte, statt der genauen Darstellung des Ortes nur die jeweilige Stadt anzugeben. Eine Einschränkung des Zugriffs auf die Standortinformationen eines Nutzers geschieht in vielen Fällen nur durch die Definition von Nutzer-Whitelists oder -Blacklists, die angeben, welche Mitglieder eines Dienstes beziehungsweise Teile des sozialen Netzwerkes eines Nutzers die Informationen sehen dürfen.

3.3.3.2 Standortnutzung auf mobilen Geräten

Fischer et al. [95] untersuchten die app-spezifische Nutzung der Ortungsdienste von iPhone-Nutzern. Viele ihrer Teilnehmer gewährten mindestens zwei Dritteln ihrer Apps Zugriff auf ihren Standort. 15 % der Teilnehmer erlaubten dies allen Apps und einer von 273 Teilnehmern erlaubte es keiner. Ein nennenswerter Anteil der Nutzer gewährte jedoch weniger als der Hälfte ihrer Apps den Zugriff auf Ortsinformationen. Dies stützt die Vermutung, dass die Nutzer verschiedene Privatsphäre-Wahrnehmungen haben und basierend auf dieser entscheiden. Innerhalb der 25 am häufigsten genutzten Apps fanden Fischer et al. deutliche Unterschiede: Während

98 % der Nutzer der *Foursquare*-App und 97 % der Nutzer der App *Karten* den Zugriff auf die Ortungsdienste gewährten, taten dies beispielsweise nur 59 % der Nutzer bei der *IMDb*-App und 53 % der Nutzer der App *Shazam*. Die Nutzer gewährten Apps mit einem deutlichen Ortsbezug häufiger die Standortabfrage. Zumindest ein Teil der Nutzer achtet darauf, welcher Natur eine App ist.

Porter Felt et al. [130] untersuchten die Wahrnehmung der Nutzer über 99 Risiken assoziiert mit 54 Berechtigungen mobiler Betriebssysteme. Sie erweitern damit die bis dato häufig auf Ortsinformationen fokussierte Sicht auf Risiken mobiler Geräte. Basierend auf den Antworten ihrer Teilnehmer erstellten sie ein Ranking der Risiken, „dass eine App etwas tut, ohne den Nutzer zuvor zu fragen“. Die Teilnehmer gaben dabei ihr Gefühl von *gleichgültig* bis *sehr verärgert* an. Im Vergleich zu Top-Risiken wie dem Löschen aller Kontakte oder dem Versenden von Premium-SMS wurde die Preisgabe von Ortsinformationen als mittelschweres Risiko eingestuft. Die Preisgabe von Ortsinformationen rangierte je nach Publikum auf den Plätzen 52 (öffentlich), 66 (Werbeanbieter), 73 (Freunde) oder 96 (App-Anbieters Server). Bei einem Ranking aller 11 betroffenen Arten von Daten befanden sich Ortsinformationen auf dem vorletzten Platz. Die Autoren zeigen, dass Ortsangaben ein Risiko darstellen, es jedoch auch andere deutliche Risiken auf den heutigen mobilen Geräten gibt.

3.3.3.3 Weitere Studien

Standortverschleierung nutzen Brush et al. [80] untersuchten die Teilnehmer-Wahrnehmung von Verschleierungsmethoden für Bewegungsprofile und inwieweit ihre Teilnehmer bereit waren, die durch diese anonymisierten Ortsinformationen zu veröffentlichen. Über einen Zeitraum von zwei Monaten zeichneten sie Bewegungsprofile ihrer Teilnehmern mittels GPS-Trackern auf und untersuchten in anschließenden Interviews, welche Verschleierungsmethoden die Teilnehmer bei der Preisgabe gegenüber verschiedenem Publikum anwenden würden. Sie verglichen das Entfernen von privaten Orten aus den Bewegungsprofilen, das Hinzufügen weiterer Punkte mittels gaußschem Rauschen, die Abbildung auf ein gröberes räumliches Raster, die Abbildung auf ein gröberes zeitliches Raster und das Entfernen von Genauigkeit um k-Anonymität zu gewährleisten. Für jede Methode konnten die Teilnehmer aus vier Ungenauigkeitsstufen wählen. 47 % Teilnehmer bevorzugten k-Anonymität, 25 % das Entfernen von privaten Orten, 22 % das Hinzufügen von Rauschen und 6 % die Abbildung auf ein grobes räumliches Raster. Die Interviews zeigten, dass die Teilnehmer anhand der Erklärungen und ihrer verschleierten Bewegungsprofile fähig waren, die Verschleierungsmethoden zu verstehen. Die Auswirkungen der verschiedenen Ungenauigkeitsstufen auf die vollständigen Bewegungsprofile schienen jedoch nicht bei allen Methoden verstanden worden zu sein. Dies zeigt das begrenzte Verständnis der Nutzer für verschiedene Verschleierungsmethoden.

Kulturelle Unterschiede Wang et al. [146] untersuchten die Unterschiede der persönlichen Einstellungen und des Verhaltens in Bezug auf Privatsphäre zwischen amerikanischen, chinesischen und indischen Nutzern Sozialer Onlinenetzwerke. Mit ihrer Vergleichsstudie zeigen sie, dass es deutliche Unterschiede zwischen diesen Ländern, die als Proxys für Kulturen dienten, gibt. In den Fällen, dass andere Personen geteilte Informationen sehen können, wie sie diese missbrauchen können und dem generellen Vertrauen in die Anbieter Sozialer Onlinenetzwerke waren am meisten die amerikanischen Teilnehmer um ihre Privatsphäre besorgt, gefolgt von den chinesischen Nutzern und zuletzt von den indischen. Im Fall von Ortsangaben mit der Genauigkeit „Straße“ empfanden beispielsweise circa 70 % der amerikanischen, circa 35 % der chinesischen und circa 15 % der indischen Teilnehmer deren Verbreitung als sehr unangenehm. Interessanterweise war das beobachtete Muster der Nationen im Fall des Wunsches den Zugriff auf Informationen einschränken zu können umgekehrt.

Crowd-unterstützte Ansätze Lin et al. [122] kombinierten eine App-Analyse mittels TaintDroid mit einer Nutzererhebung durch Crowdsourcing, um Differenzen zwischen der erwarteten und der wirklichen Datennutzung von Apps zu erfassen. Zu 100 betrachteten Apps erfragten sie die Einschätzung von Nutzern darüber, ob die Apps auf ausgewählte persönliche Informationen wie auch den aktuellen Aufenthaltsort zugreifen. Sie ließen die Nutzer zudem vermuten, wieso eine App die jeweiligen Informationen verwendet. Außerdem bewerteten die Nutzer, wie es ihnen behagt, der App Zugriff auf die Informationen zu gewähren. In einer Vergleichsgruppe erfassten die Autoren, wie die Nutzer die Verwendung der persönlichen Informationen empfanden, wenn sie detaillierte Informationen über den Zweck der Verwendung erhielten (wie Hauptfunktion, Zusatzfunktion oder personalisierte Werbung). Diese waren zuvor durch die App-Analyse ermittelt worden. Die Studie zeigt, dass sich die Teilnehmer wohler fühlten, wenn sie genauere Informationen über den Verwendungszweck persönlicher Daten erhielten. Der Vergleich der Ergebnisse beider Gruppen zeigte, wie die Erwartungen der Nutzer von der Realität abwichen. Die ermittelte Diskrepanz verwendeten Lin et al. im Weiteren als Basis für eine modifizierte Privatsphäre-Übersicht im Rahmen der Installation von Apps unter Android: Diese präsentiert Nutzern die erfasste Verwunderung anderer Nutzer über das Verhalten einer App als Basis für die Entscheidungen, ob sie die App installieren oder nicht. Während die Teilnehmer ihrer Studie über Amazon Mechanical Turk rekrutiert wurden, beschreiben Lin et al. als Langzeitziel ihrer Arbeit, ein System zu entwickeln, das Crowdsourcing und App-Analyse kombiniert, um das Verhalten von Apps und die Abweichung von den Erwartungen der Nutzer zu erfassen. Diese Informationen sollen helfen, den Schutz der Privatsphäre zu verbessern.

Kapitel 4

Bedrohungsanalyse

Durch die Preisgabe persönlicher Informationen einer Person kann Schaden für die Privatsphäre der Person entstehen. Eine solche Störung des privaten Bereichs kann Ärgernisse oder Schamgefühle entstehen lassen und kann sogar letztendlich auch zu Schaden für das leibliche Wohl führen. Aus diesem Grund ist jegliche Preisgabe von persönlichen Informationen als mögliche Bedrohung der Privatsphäre zu sehen und sollte nur bedacht geschehen. Auch wenn eine Information allein nicht als bedrohlich wahrzunehmen ist, kann sie gebündelt mit anderen zu einer Bedrohung werden.

Zu Zeiten des klassischen Webs waren vor allem Firmen diejenigen, die als Quelle von Bedrohungen der Privatsphäre in der Welt der IT ausgemacht wurden, weil sie Informationen über Nutzer und ihr Verhalten sammelten. Die Nutzer waren zu diesem Zeitpunkt Konsumenten von Webangeboten und lediglich Opfer. Seit dem Aufkommen des Web 2.0 und des Social Webs geben die Nutzer jedoch von sich aus sehr viel von sich und sogar Anderen preis. Sie teilen persönliche Informationen mit Anderen und der Öffentlichkeit. Durch das Teilen der Informationen sind heute nicht nur Firmen die Quelle von Bedrohungen. Quasi jeder andere Nutzer des Social Webs kann auf Basis preisgegebener Informationen eine Bedrohung entstehen lassen, unabhängig davon, ob als Privatperson, im Kontext der Berufswelt oder dem Kontext anderer Lebensbereiche. Betrachtet man heute Bedrohung der Privatsphäre, muss daher der Fokus auch auf das Preisgeben von Informationen durch die Nutzer und den Informationsgehalt veröffentlichter Information gelegt werden und nicht nur auf das Sammeln persönlicher oder personenbezogener Informationen durch Institutionen. Dies beides steht im Fokus dieser Dissertation, die sich mit dem Bewusstsein über preisgegebene Informationen und über die aktive Preisgabe auseinandersetzt.

Die Preisgabe von persönlichen Informationen ist zu differenzieren in die böswillige, die unbeabsichtigte und die beabsichtigte Preisgabe. Die böswillige Preisgabe geschieht durch jemand anderen als die betroffene Person. Hat diese Person Zugriff auf persönliche Informationen, kann sie diese in böswilliger Absicht zum Schaden der betroffenen Person weitergeben oder öffentlich machen. Der böswilligen Preisgabe

kann ein Diebstahl der Informationen vorausgehen. Dies ist mehr ein Problem der IT-Sicherheit und wird hier nicht weiter betrachtet.

Des Weiteren kann eine betroffene Person selbst oder jemand anderes Informationen unbeabsichtigt preisgeben, was im Sinne der betroffenen Personen nicht geschehen sollte. Ein Grund hierfür kann beispielsweise Unaufmerksamkeit oder Naivität sein. Eine besondere Form der unbeabsichtigten Preisgabe ist die unbewusste Preisgabe: Die preisgebende Person respektive die betroffene Person ist sich in diesem Fall nicht bewusst, dass persönliche Informationen preisgegeben werden oder schon preisgegeben worden sind. Die immer weiter steigende Vielfalt und damit verbundene Komplexität unseres technisierten Alltags sorgt dafür, dass Preisgaben von persönlichen Informationen mit einer steigenden Tendenz unbewusst geschehen, da es für den Nutzer und vor allem für Laien quasi unmöglich ist, zwischen allen technischen Details den Überblick über die Verwendung, die Weitergabe und die Veröffentlichung der persönlichen Informationen zu wahren.

In Software, in mobilen Apps und in Webdiensten wie dem Sozialen Onlinenetzwerk Facebook finden sich heute hinter der Bezeichnung Privatsphäre-Einstellungen meist Funktionen, die Nutzern die Kontrolle über die Preisgabe von Informationen geben sollen. Diese schaffen vorwiegend Kontrolle über eigene persönliche Informationen durch die kontrollierte Nicht-Preisgabe offensichtlicher und direkt genannter Informationen, wie selbst geteilter Fotos oder persönlicher Daten des eigenen Profils. Einer unbewussten Preisgabe von Informationen wirken sie jedoch nicht entgegen. Zum Schutz gegen die wachsende Bedrohung durch eine unbewusste Preisgabe existieren bisher wenig Hilfen. Hier muss in erster Linie Bewusstsein über die Existenz persönlicher Informationen geschaffen werden, um im Weiteren Hilfestellungen zur Kontrolle der Weitergabe oder Veröffentlichung geben zu können.

Auch eine betroffene Person selbst kann persönliche Informationen bewusst preisgeben. Hier finden sich die Personen wieder, die kein Interesse oder kein Gespür für die Privatheit persönlicher Informationen besitzen. Dieser Aspekt wird im Rahmen dieser Arbeit nicht betrachtet. Jedoch verbreitet sich seit einigen Jahren eine Art der bewussten Preisgabe in der Praxis, die im Rahmen dieser Arbeit aus eher technischer Sicht berücksichtigt wird: die billigende Preisgabe von persönlichen Informationen. Viele Angebote in Form von Webdiensten oder mobilen Apps bieten heute Funktionen auf Basis persönlicher Informationen an. Will ein Nutzer solch eine kontextsensitive Funktion nutzen, so muss er sich in der Regel entscheiden, ob er das Geforderte von sich preisgibt oder auf die Funktion verzichtet. Die Nutzer entscheiden situationsbedingt auf Basis einer persönlichen Abwägung, ob die Funktion ihnen wichtiger ist oder die ihnen bekannten Risiken einer Preisgabe überwiegen. Problematisch ist dabei, dass den Nutzern nur begrenzt bewusst ist, welche Informationen mit welchem Detailgrad letztendlich preisgegeben werden, und ob dies für die angestrebte Funktion überhaupt notwendig ist.

4.1 Bedrohungen durch geteilte Fotos

Eine Vielzahl von Bedrohungen der Privatsphäre entsteht durch die Preisgabe von persönlichen Informationen im Kontext von Social Media. Der Fokus dieser Arbeit richtet sich dabei auf geteilte Fotos.

Lediglich auf einem Foto im Web abgebildet zu sein ist für einige Menschen schon ein Grund zur Besorgnis. Selbst wenn sie das Bild an einem absolut unbedenklichen Ort in einer ebenso harmlosen Situation zeigt, können solche Fotos Bedenken bei einer abgebildeten Person erzeugen. Entsprechend stärkeres Unbehagen und deutlichere Bedrohungen der Privatsphäre einer Person entstehen, wenn Bilder jemanden in einer Situation oder an einem Ort zeigen, die von Einzelnen oder allgemein von der Gesellschaft als verwerflich oder unangemessen empfunden werden. Fotos von betrunkenen Personen, Fotos von kriminellem Handeln wie vom Drogenkonsum, Fotos von unangemessen gekleideten Personen oder Fotos, die jemanden in einer als nicht angemessen empfundenen Gesellschaft zeigen, sind hier häufig genannte Beispiele. Besonders zu Beginn der Verbreitung von Sozialen Onlinenetzwerken haben eben solche Bilder für unachtsame Nutzer in der Realität schon zu Problemen geführt.

Wissenschaftliche Untersuchungen haben gezeigt, dass die von Menschen empfundene Bedrohung der Privatsphäre von jeder anderen Person ausgehen kann. Sowohl Familienmitglieder, Freunde und andere Personen im unmittelbaren persönlichen Umfeld eines Menschen [77], als auch entfernt bekannte bis hin zu unbekannten Personen [71, 138] werden als Quelle für Bedrohungen empfunden. Beides hat sich in der Vergangenheit schon in der Praxis gezeigt. Neben Ärger oder Rufschaden im persönlichen Umfeld haben geteilte Inhalte auch schon zu Auswirkungen auf das Berufsleben oder die finanzielle Lage von Menschen geführt, wie Presseberichte dokumentierten und diskutierten.

Die Zeit berichtet im September 2009 von einer Studie im Auftrag des Bundesverbraucherschutzministeriums, laut der „mehr als ein Viertel der Unternehmen ihre Bewerber auch über das Netz bei der Jobvergabe durchleuchten“ und „gut ein Drittel der Firmen schaut auch in die Profile von sozialen Netzwerken wie Facebook oder StudiVZ“ [54]. Über ähnliche Probleme in den USA berichtete die New York Times schon im Juli 2006 [48]. Auch bei der Aufnahme eines Kredites können im Web geteilte Informationen zum Problem werden. Nachdem im Jahr 2012 ursprünglich die Wirtschaftsauskunftei *Schufa* Auskünfte zur Kreditwürdigkeit auch auf Basis von Social-Media-Inhalten geben wollte und so für Furore in der Öffentlichkeit sorgte, verfolgen nun andere Firmen diese Strategie und bieten entsprechende Auskünfte an [30], wie es schon zwei Jahre zuvor in den USA der Fall gewesen ist [46]. Auch Versicherungen nutzten Social Media, um sich über Versicherte zu informieren. So wurden im Jahr 2009 in Kanada [8] und im Jahr 2011 in den USA [25] Versicherungsleistungen aufgrund geteilter Fotos gestrichen. Im Jahr 2010 be-

richtete der Spiegel über Untersuchungen in den USA, die das Ziel verfolgten, die Bewertung von Krankheitsrisiken oder der Risikobereitschaft von Versicherten auf Basis von Marktforschungsdaten und Informationen aus dem Web [40] vorzunehmen. So könnten freiwillig im Web geteilte Essgewohnheiten oder die preisgegebene Affinität zum Sporttreiben medizinische Untersuchungen und die Befragung der Personen ergänzen. Jedoch könnten geteilte Informationen zu ungesundem Essen oder geteilte Fotos vom Betreiben von Risikosportarten auch negative Auswirkungen auf geforderte Versicherungsbeiträge zur Folge haben.

Pressemeldungen dieser Art haben in den vergangenen Jahren dafür gesorgt, dass ein Teil der Menschen bedachter mit der öffentlichen Preisgabe von persönlichen Informationen im Web, wie auch dem Teilen von Fotos in Sozialen Onlinenetzwerken, umgeht. Neben einer gewissen Selbsteinschränkung, was die Menschen im Web teilen, dienen heute vor allem die Zugriffsschutzmechanismen der Onlinedienste dazu, den Zugriff auf geteilte Inhalte einzuschränken. Diese helfen jedoch nur, einen geringen Anteil der Probleme zu mildern.

4.1.1 Zugriffsschutz

Zugriffsschutzmechanismen erlauben Nutzern innerhalb von Sozialen Onlinenetzwerken und Online-Communitys die Beschränkung, wer welche ihrer geteilten Inhalte sehen darf. Für einzelne Fotos oder ganze Alben erlauben diese eine Zugriffseinschränkung von öffentlich über sichtbar für definierbare Gruppen von Kontakten bis hin zur Beschränkung auf den Nutzer selbst. Die Praxis zeigt jedoch, dass diese Mechanismen nicht immer ausreichend die Wünsche der Nutzer abbilden können oder die gebotenen Möglichkeiten aufgrund der Komplexität und des Verwaltungsaufwandes nicht ausgeschöpft werden. Während der Zugriff innerhalb dieser Communitys auf registrierte Nutzer beschränkt ist, erlauben andere Anbieter, wie beispielsweise Cloud-Speicher-Dienste das Teilen über die Weitergabe geheimer Webadressen, so dass das Wissen über eine Webadresse einer Zugriffserlaubnis gleichkommt.

Unabhängig von der Umsetzung dienen alle Arten von Zugriffsschutz jedoch ausschließlich der Beschränkung des Publikums der Informationen, die ein Nutzer bewusst selbst teilt.

4.1.2 Verursacher und Betroffene

Bedrohungen der Privatsphäre durch geteilte Bilder lassen sich in zwei Kategorien gliedern, abhängig davon, wie die durch ein Bild betroffenen Personen in den Prozess des Teilens involviert sind. Eine Person gilt hierbei als betroffen, wenn sie auf einem Bild abgebildet ist oder in irgendeiner anderen Weise mit dem Bild in Verbindung gebracht werden kann.

Selbstverursachte Bedrohungen entstehen durch Bilder, die von den betroffenen selbst hochgeladen werden. Ein Beispiel für eine Bedrohung der Privatsphäre könnte hier sein, dass ein Nutzer ein Foto von sich selbst hochlädt und es in Hinblick auf seine aktuelle Lebenssituation mit einem unzureichenden Zugriffsschutz versieht oder es mit unzureichend Voraussicht schützt und in der Zukunft jemand ungeplant auf dieses Foto stößt. In Sozialen Onlinenetzwerken kann dies passieren, indem ein Nutzer ein Foto in einem teilöffentlichen Album statt in einem privaten teilt oder es sogar öffentlich in seiner persönlichen Chronik präsentiert. Dies sind die Fälle, in denen Zugriffsschutz ein passendes Mittel zum Schutz der Privatsphäre ist, jedoch muss er dazu richtig eingesetzt werden. Die Möglichkeit der Beeinträchtigung der Privatsphäre und mögliche Folgen sind in diesem Fall offensichtlich und können relativ schnell eintreten, da eine direkte Verbindung zwischen einem schädigenden Bild und der betroffenen Person existiert. Eine schnelle Problementstehung wird vor allem dadurch provoziert, dass das Publikum (die Online-Freunde, oft auch inklusive der eigenen Familie) eine direkte Verbindung zur betroffenen Person hat und so persönlich motivierte Probleme entstehen können. Eher längerfristig können Probleme durch entfernt Bekannte oder Fremde entstehen, wie in den zuvor genannten Beispielen zu Arbeitgebern, Banken oder Versicherungen.

Eine Besonderheit, die Probleme auf Basis selbst geteilter Bilder auszeichnet, ist der Wandel des Verständnisses, was ein Nutzer selbst sowie auch Andere als unpassend und schädigend empfinden. Dies ist ein ernstzunehmendes Problem, welches vor allem die *Generation Facebook* betraf, die ihre Jugend oder ihr junges Erwachsenenalter zeitgleich mit dem Entstehen der Sozialen Onlinenetzwerke durchlebten und viele prekäre Details ihres Privatlebens mit Anderen oder öffentlich teilten. Dies heute zu verhindern ist Aufgabe der Aufklärung im Rahmen der Erziehung und der Vermittlung von Medienkompetenz. Selbstverschuldete Bedrohungen durch die Motive geteilter Bilder werden in dieser Dissertation nicht weiter vertieft.

Die zweite Kategorie bilden fremdverursachte Bedrohungen. Sie entstehen durch Bilder, die von anderen als den betroffenen Personen hochgeladen werden. Mit dem massenhaften Teilen im Web stellen diese Bilder eine wachsende Bedrohung der Privatsphäre dar. Die hochladenden Personen reichen dabei von Freunden bis hin zu völlig fremden Menschen und entsprechend vielfältig sind die Szenarien in denen Bedrohungen geschaffen werden. Beispielsweise kann ein alter Freund Erinnerungen an sein Studium in Form von Fotos mit anderen teilen. Diese Fotos zeigen ehemalige Kommilitonen, zu denen er keinen Kontakt mehr hat, in deren Interesse es jedoch wäre von der Veröffentlichung der Bilder zu erfahren. Wohl noch häufiger teilen jedoch fremde Personen Fotos, von denen die Betroffenen nicht wissen. Macht jemand beispielsweise Fotos in der Öffentlichkeit, so sind häufig unbekannte Personen im Hintergrund abgebildet. Solch ein Foto könnte, sollte es von einer dritten Per-

son entdeckt werden, die die fotografierte Person kennt, eine Bedrohung für deren Privatsphäre entstehen lassen.

Bedrohungen der zweiten Kategorie sind besonders problematisch, da die Betroffenen nicht in den Prozess des Hochladens der Bilder und die Preisgabe von Informationen involviert sind. Ferner können sie das Hochladen nicht verhindern oder zeitnah etwas gegen die geteilten Bilder unternehmen, solange sie nicht von ihnen wissen. Zuallererst muss die betroffene Person von einem entsprechenden Bild erfahren. Jedoch selbst dann bieten Onlinedienste heute kaum eine Möglichkeit, sich gegen ein Bild zu schützen, außer im Nachhinein Beschwerde beim Teilenden oder beim Dienstbetreiber zu erheben oder rechtliche Schritte einzuleiten. Insbesondere hat der Betroffene keinen Einfluss darauf, wer sonst das Bild schon zu Gesicht bekommen hat und eventuell sogar dupliziert hat.

Da das Hochladen von Bildern der zweiten Kategorie nicht verhindert werden kann, ist das Bewusstsein über solche Bilder eine grundlegende Voraussetzung, um sich gegen Bedrohungen durch diese schützen zu können. Dabei stellt sich die Herausforderung, die Bilder zu finden, die einen Nutzer betreffen, da ein Großteil der geteilten Bilder keine Relevanz für ihn hat.

4.1.3 Voraussetzungen für eine Bedrohung

Damit ein Bild Grundlage einer Bedrohung für eine Person werden und Schaden für diese verursachen kann, müssen folgende Voraussetzungen gegeben sein.

1. Für beide zuvor beschriebenen Kategorien von Bildern/Bedrohungen gilt, dass ein Bild schädlichen Inhalt besitzen muss, um die Privatsphäre zu stören oder der Person zu schaden. Schädlicher Inhalt kann in zwei Formen auftreten:

   (a) Der Bildinhalt kann die Person in einer unpassenden Situation oder auf eine unpassende Weise darstellen.

   (b) Zusatzinformationen in Form von integrierten oder mit dem Bild angezeigten Metadaten können schädlichen Inhalt darstellen, indem sie beispielsweise die Zeit, den Ort, oder Namen anderer beteiligter Personen preisgeben. Ferner kann eine Bildunterschrift oder ein Kommentar einer dritten Person auch schädlich sein.

2. Für die im Rahmen dieser Arbeit vorwiegend betrachtete zweite Kategorie von Bildern – die durch Andere hochgeladenen Bilder – muss außerdem eine Verbindung zwischen dem Bild und der Person hergestellt werden können. Dies kann wiederum auf zwei Arten geschehen:

   (a) Die Person wird durch jemand anderen erkannt. Derjenige kann die Verbindung auch Dritten gegenüber preisgeben.

(b) Durch Zusatzinformationen wird eine Verbindung zwischen dem Bild und der Person hergestellt. Dies kann eine Hypertext-Verknüpfung mit einer Profilseite innerhalb eines Onlinedienstes sein. Auch kann es die Speicherung des Namens der Person innerhalb integrierter oder mit dem Bild angezeigter Metadaten sein.

4.1.4 Bewusstsein über bedrohliche Bilder

Die weitverbreiteten Sozialen Onlinenetzwerke und einige Foto-Communitys ermöglichen Nutzern, Objekte und andere Personen in geteilten Bildern zu markieren. Namen können in der Beschreibung oder in Kommentaren zu einem Bild verwendet werden oder Gesichter direkt im Bild markiert und mit Namen annotiert werden. Typischerweise erstellen diese Markierungen, insofern es sich bei den markierten Personen um Mitglieder des sozialen Netzwerkes der markierenden Person handelt, eine direkte Hypertext-Verknüpfung mit dem Profil der markierten Person. Dies ermöglicht es Anderen vom Bild direkt zum Profil der Person zu gelangen oder auch anders herum vom Profil zu Bildern einer Person zu gelangen. Die Einführung dieser Art von Personen-Markierungen verursachte innerhalb kurzer Zeit eine Menge öffentlicher Kritik und Diskussionen über mögliche Beeinträchtigungen der Privatsphäre der Markierten: Offensichtlich erleichterten die Verknüpfungen den Zugriff auf persönliche Informationen der Abgebildeten genauso wie den Zugriff auf zum Teil beschämende oder schädliche Bilder. Aus diesem Grund führten Dienste wie Facebook schnell Privatsphäre-Einstellungen ein, die Nutzern erlaubten, das Markieren ihrer Person durch Andere zu verbieten oder sich alternativ automatisch über Markierungen informieren zu lassen, um diese aktiv zu moderieren: Sobald ein Nutzer über eine Markierung informiert wird, kann er im Folgenden die Verknüpfung verneinen oder entfernen und ebenfalls in Erwägung ziehen, das Foto löschen zu lassen oder, wie verwandte wissenschaftliche Arbeiten [78, 136] vorschlugen, die Sichtbarkeit des Bildes einschränken zu lassen. Durch die Benachrichtigung der Markierten schaffen die profilverknüpften Markierungen einen gewissen Grad an Bewusstsein.

Unter dem Gesichtspunkt über bedrohliche Fotos informiert zu sein, ist eine eher als Bedrohung zu betrachtende Art markiert zu werden, die Markierung ohne Profilverknüpfung und ohne Benachrichtigung. Einige Dienste erlauben, Freitext-Markierungen auf Bildern zu setzen. In diesen können ebenso wie in Kommentaren zu einem Bild Namen oder andere identifizierende Merkmale durch die hochladende Person oder Dritte eingetragen werden. So können sowohl Personen markiert werden, die selbst Nutzer des Dienstes sind, jedoch auch solche, die keine Mitnutzer sind. Die Integration von entsprechenden Metadaten in hochgeladenen Bilddateien kommt diesem Szenario der Onlinedienste gleich. Die durch diese Art der Markierung entstehende Bedrohung unterscheidet sich deutlich von der vorherigen. Die Wahr-

scheinlichkeit einer unmittelbaren Bedrohung oder sogar Schadens ist geringer, da auch die Personen, die einen Bezug zur markierten Person besitzen, nicht direkt vom jeweiligen Bild erfahren. Eine potenzielle Bedrohung bleibt jedoch wie auch das Bild selbst weitaus länger vor der markierten Person verborgen. Die betroffene Person selbst kann unwissend über ein Bild bleiben, während jemand der aktiv nach Informationen über die Person sucht das Bild finden kann, spätestens dann, wenn Suchmaschinen diese Art von Metadaten beginnen großflächig zu indexieren.

Alle übrigen Bilder, die Personen zeigen jedoch gar keine Markierungen enthalten, können ebenso bedrohlich sein, wenn auch die Wahrscheinlichkeit einer Bedrohung zumindest heute noch geringer ist. Ohne jegliche Verbindung zu einer betroffenen Person kann solch ein Foto nur eine Gefahr darstellen und Schaden verursachen, wenn jemand der die betroffene Person kennt, auf ein entsprechendes Foto stößt, die Person erkennt und so eine Verbindung herstellt. Während die Wahrscheinlichkeit, dass dies passiert und zu Schaden führt, heute gering ist, ist es jedoch möglich.

Wie unwahrscheinlich Bedrohungen durch Bilder ohne offensichtliche Markierung auch sind, genauso schwierig ist es, auf diese aufmerksam zu werden. Die einzige Möglichkeit besteht momentan in der aktiven manuellen Suche nach solchen Bildern.

4.1.5 Lebensdauer und Wirkungsbereich

Betrachtet man die Lebensdauer von Social-Media-Inhalten, so muss man zwischen der Sichtbarkeit, der Auffindbarkeit und der Speicherung der Informationen differenzieren. Über die Dauer der Speicherung können nur die Dienstanbieter selbst Angaben machen. Die Sichtbarkeit und Auffindbarkeit von Informationen ist unabhängig von ihr und ist vielmehr durch die Funktionen und Visualisierung der Nutzerschnittstellen beschränkt. So war beispielsweise in den ersten Jahren des Dienstes Twitter die im Web sichtbare Historie von Mikroblog-Beiträgen begrenzt. Heute hingegen kann selbst ein Nutzer der ersten Stunde bis zu seinem ersten Beitrag zurückgehen. Spätestens seit dem konzeptionellen Umbau von der *Pinnwand* eines Nutzers zu seiner *Chronik* gilt dieses ebenso für das Soziale Onlinenetzwerk Facebook. Dass ein Beitrag für einen Nutzer nicht mehr auffindbar ist, bedeutet nicht, dass er auch nicht mehr gespeichert ist. Und Gleiches gilt für die Sichtbarkeit: Wird mit den aktuellen Nutzerschnittstellen ein älterer Beitrag nicht dargestellt, so bedeutet dies weder, dass sich dies später nicht ändern könnte, noch dass jemand, der aktiv sucht, die Informationen mit entsprechendem Know-how beispielsweise über eine Programmierschnittstelle nicht finden könnte.

Gleiches gilt für im Web geteilte Bilder. Besonders in den Fällen, wenn Bilder nicht in übersichtlichen Fotoalben abgelegt werden, sondern über eher schnelllebige Mechanismen wie die genannten Beispiele geteilt werden.

Ein weiterer Aspekt, der einen Einfluss auf die Bedrohung durch geteilte Bilder

hat, ist der Wirkungsbereich von geteilten Inhalten. Werden Fotos in einem Sozialen Onlinenetzwerk geteilt, so sorgen in erster Linie Zugriffsschutzmechanismen dafür, dass nur berechtige Mitnutzer Inhalte wie Bilder sehen dürfen. In zweiter Linie wird das Publikum auch durch die notwendige Mitgliedschaft und den Login bei einem solchen Dienst beschränkt. Andere Dienste, wie beispielsweise die Foto-Community Flickr sehen hingegen vor, dass Bilder auch über die Grenzen des Dienstes hinweg öffentlich im Web geteilt werden können. Dies bedeutet nicht, dass das öffentliche Teilen in Ersteren weniger problematisch und bedrohlich sein kann. Vielmehr müssen beim Letzteren weitere Nebeneffekte betrachtet werden. So kann nicht nur jeder Nutzer auf die Inhalte zugreifen, sondern auch Suchmaschinen, die Inhalte wie die Bilder und prinzipiell auch deren Metadaten indexieren und für die Suche nutzbar machen könnten. Ebenso ist bei Letzteren das Duplizieren von Inhalten für eine breitere Masse möglich.

In Bezug auf den Wirkungsbereich und die Lebensdauer geteilter Bilder sind insbesondere auch deren Metadaten zu betrachten, welche das Bedrohungspotenzial maßgeblich erhöhen können. Die Art der Speicherung spielt bei diesem Aspekt eine entscheidende Rolle. Werden Metadaten innerhalb eines Dienstes annotiert, wie beispielsweise bei der Markierung einer Person inklusive Namen, und vom Dienst selbst in seiner Datenbank gespeichert, so ist der Zugriff auf diese Informationen auch nur über den Dienst beziehungsweise innerhalb des Dienstes möglich. Wird ein Foto dupliziert, weitergeleitet oder anderenorts nochmals veröffentlicht, so werden die Metainformationen nicht dupliziert. Diese müssen mit entsprechendem Mehraufwand ebenfalls dupliziert werden. Werden Metadaten hingegen in Bilddateien integriert, so werden diese mit dem Bild selbst dupliziert, kopiert und vervielfältigt, solange sie nicht expliziert entfernt werden.

4.1.6 Bedrohungen durch Bild-Metadaten

Während es mit dem heutigen Stand der Technik immer noch schwierig ist, große Mengen von Bildern allein auf Basis der Motive zu durchsuchen, um beispielsweise Informationen zu einem Ort oder zu einer Person zu sammeln, helfen Metadaten dabei, die schwer zu durchsuchenden Informationen zu beherrschen. Metadaten bieten die Möglichkeit, Bilder einfacher zu sortieren oder zu durchsuchen. Dies ist in vielen Situationen von Vorteil, jedoch bergen Metadaten aus denselben Gründen auch Bedrohungen für die Privatsphäre. Wie zuvor beschrieben wurde, müssen zwei Voraussetzungen erfüllt sein, damit ein Bild zu einer Bedrohung der Privatsphäre werden kann. Bild-Metadaten können beide Voraussetzungen erfüllen und so zur Grundlage für eine Bedrohung der Privatsphäre werden: Sie können die Verbindung zwischen einer Person und einem Bild herstellen (Betroffensein). Sie können ebenso weitere Informationen über das abgebildete Motiv (schädlichen Inhalt) enthalten.

4.1.6.1 Dienstinterne Metadaten

Viele Dienste im Web, die das Teilen von Fotos ermöglichen, erlauben auch das Hinzufügen von Metainformationen zu den geteilten Bildern.

In den meisten Fällen geschieht das Hinzufügen manuell: Nutzer fügen auf der Webseite des Dienstes, über eine Client-Anwendung am PC oder über eine App auf einem mobilen Gerät Informationen zu einem Bild hinzu, während sie es hochladen oder nachdem sie es hochgeladen haben. Meist können auf diese Weise ein Titel, eine Bildbeschreibung, Schlagworte und sogar der Ort einer Aufnahme hinzugefügt werden. Viele Social-Media-Dienste erlauben ferner auch, Bilder anderer zu annotieren. So können Kommentare hinzugefügt werden oder Personen im Bild markiert werden. Die verschiedenen Dienste unterscheiden sich dabei vor allem im Detail: So können Orte durch eine Eingabe oder Auswahl von Ortsnamen oder durch die Angabe genauer Koordinaten spezifiziert werden. Personen-Markierungen können auf die Mitglieder des sozialen Netzwerkes eines Nutzers beschränkt sein oder es kann beliebiger Text beigefügt werden.

Neben der rein manuellen Eingabe von Kontextinformationen unterstützen einige Anwendungen den Nutzer bei der Eingabe. So nutzen einige Apps den GPS-Empfänger eines mobilen Gerätes, um den aktuellen Standort als Ort einer im Hochladen befindlichen Aufnahme vorzuschlagen. Andere schlagen sogar Personen zur Markierung vor [14]. Enthalten Fotos eingebettete Metadaten, so erlauben einige Anwendungen die Übernahme der Informationen als dienstinterne Metadaten.

Das manuelle Hinzufügen von Kontextinformationen innerhalb von Webdiensten ist eine bewusste Handlung der hinzufügenden Personen. Somit ist zumindest diesen bewusst, welche Informationen zu einem Bild gespeichert werden. Sind jedoch andere Personen von einem Bild betroffen, erfahren diese nur unter Umständen von den Informationen. Metadaten, die innerhalb eines Dienstes gespeichert werden, bieten aus der Perspektive des Privatsphäreschutzes den Vorteil, dass sie eng mit einem Dienst gekoppelt sind. Auf sie kann in der Regel nur über den Dienst oder über entsprechende Programmierschnittstellen zugegriffen werden, so dass die Zugriffsschutzmechanismen des Dienstes einen gewissen Schutz für diese bieten.

4.1.6.2 Eingebettete Metadaten

Metadaten, die innerhalb von Bilddateien gespeichert werden, decken heute eine Vielzahl von Kontextinformationen ab. Gespeichert werden die Informationen auf Basis der aktuellen Metadaten-Standards Exif, IPTC und XMP. Schließt man herstellerspezifische Metadaten mit ein, so erlauben die Standards das Speichern mehrerer Hundert Kontextinformationen. Die Zahl der potenziell eingebetteten Informationen ist somit um ein Vielfaches größer als die Eingabe in Webdiensten erlaubt.

Viele eingebettete Metadaten beinhalten lediglich technische Details zu einem

Bild, wie etwa die Brennweite des Objektivs oder die Belichtungsdauer, welche auf die Privatsphäre der Nutzer keine Auswirkung haben. Jedoch darf die Menge der privatsphärerelevanten Metadaten nicht unterschätzt werden. Unter anderem können die folgenden Informationen in einer Bilddatei eingebettet sein.

Viele Kameras und Anwendungen speichern ein **Vorschaubild** in den Metadaten, das der schnellen Ansicht der Bilder dient. Wird ein Bild beschnitten, jedoch die Vorschau danach nicht aktualisiert, können entfernte Teile des Motivs durch das Vorschaubild ungewollt preisgegeben werden.

Datum und Uhrzeit einer Aufnahme geben an, wann ein Bild erstellt worden ist und damit, wann abgebildete Personen in der dargestellten Situation waren. Insbesondere bei modernen Geräten, die ihre Uhrzeit über das Mobilfunknetz oder das Internet abgleichen, ist diese Uhrzeit als korrekt anzusehen. Lediglich die korrekte Zeitzone fehlt. Werden GPS-Angaben im Bild gespeichert, können diese auch die durch den GPS-Empfänger ermittelte Zeit einschließen, welche genau ist, die Zeitzone einschließt und durch den Kameranutzer nicht beeinflusst werden kann.

Einige Kameras erlauben den **Besitzer der Kamera** einmalig festzulegen, so dass dieser Name automatisch von der Kamera in allen Bildern gespeichert wird. Dem Besitzer kann man unterstellen, dass er am Ort des Geschehens war, auch wenn er selbst nicht abgelichtet ist.

Die **eindeutige Seriennummer einer Kamera** wird heute von einer Vielzahl klassischer Digitalkameras in allen aufgenommenen Bildern gespeichert. Diese kann auch der Identifizierung der Person des Besitzers dienen, vor allem, wenn Name des Besitzers und Seriennummer in mindestens einem Bild zusammen veröffentlicht worden sind. Die Seriennummer einer Kamera ist nicht so eindeutig wie beispielsweise die IMEI für ein Mobiltelefon, sie ist jedoch zumindest im Zusammenhang mit Kamerahersteller und Kameramodell eindeutig für ein Gerät.

Der bis dato manuell hinzugefügte **Name des Erstellers** oder der **Künstler** geben an, wer ein Bild geschaffen hat und somit auch am Ort des Geschehens war, auch wenn die Person nicht auf dem Bild zu sehen ist. Gleiches gilt für den **Urheber**, zu dem Informationen im Bild gespeichert werden können. Neben dem Namen kann auch die **Adresse** oder **Telefonnummer** des Erstellers oder einer bearbeitenden Personen gespeichert werden.

Neuere XMP-Erweiterungen wie das *Microsoft Photo Region Schema* [67] und das *Metadata Working Group Regions Schema* [66] erlauben **Personen-Markierungen** in Bildern zu speichern, wie es bisher nur aus Sozialen Onlinenetzwerken bekannt ist. Es können Namen von abgebildeten Personen gespeichert werden. Die Erweiterungen erlauben zudem, Bildausschnitte mit einem Kreis oder einem Rechteck zu markieren und so Namen eindeutig zu einer Person oder einem Gesicht zuzuordnen. Solch eine Zuordnung verleiht der Bedrohung durch Überwachungsmaßnahmen mit

Gesichtserkennung eine weitaus größere Dimension, da die Nutzer selbst unbewusst eine im Internet öffentliche Datenbank von Vergleichsbildern erstellen.

Informationen über den Ort eines Bildes können den Ort des Fotografen oder den Ort des Motivs beschreiben. Vor allem **koordinatenbasierte Ortsangaben** in Form von GPS-Koordinaten sind weit verbreitet. Jedoch können auch **textuelle Ortsangaben** den Ort beschreiben. Diese geben den Ort mit verschiedener Genauigkeit wieder: von einer Postadresse oder dem Namen einer Sehenswürdigkeit über die Stadt bis hin zum Land einer Aufnahme. Während koordinatenbasierte Angaben in der Vergangenheit häufiger in der Kritik waren, haben textuelle Ortsbeschreibungen bisher wenig Beachtung gefunden. Textuelle und koordinatenbasierte Ortsinformationen können durch Geokodierung beziehungsweise Adresskodierung mittels frei verfügbarer Webdienste durch jedermann ineinander umgewandelt werden.

Der **Titel** oder die **Beschreibung** eines Bildes erläutern das Motiv kurz und prägnant oder ausführlich. Beide können auch einen für jemanden schädlichen Inhalt in Worte fassen, der durch die Beschreibung maschinell verarbeitbar gemacht wird. Ähnliches gilt für annotierte **Schlagworte**, wenngleich diese durch ihre Kürze und Allgemeinheit häufig weniger Bedrohungspotenzial bieten.

Durch die gemeinsame Speicherung der verschiedenen Metainformationen ein einem Bild werden diese nicht nur an das Bild gebunden, sondern auch miteinander verknüpft, so dass auch durch ihr gemeinsames Auftreten eine Bedrohung der Privatsphäre entstehen kann. Welche grundlegenden Informationen auf Basis der genannten Metainformationen gewonnen werden können, fasst Abbildung 4.1 zusammen.

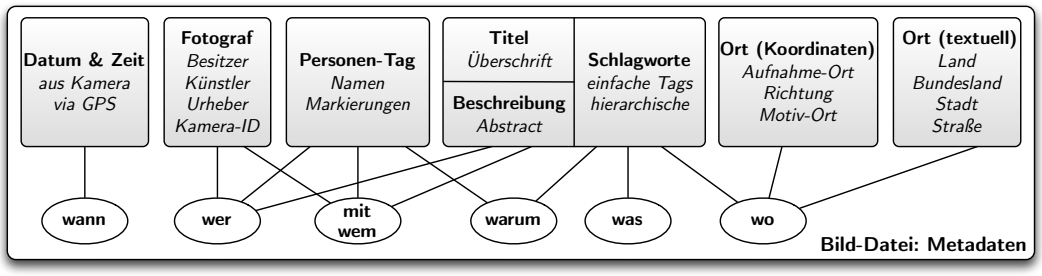


Abbildung 4.1: Integrierte Bild-Metadaten und erschließbare Informationen

Nur wenige der privatsphärerelevanten eingebetteten Metadaten wurden bis heute in der Forschung im Kontext des Privatsphäreschutzes betrachtet. Der Schutz mindestens ebenso weniger wird in Software oder in Webdiensten berücksichtigt. Nach öffentlichen Diskussionen sind in Sozialen Onlinenetzwerken Privatsphäre-Mechanismen und Optionen zu Ortsangaben und Personen-Markierungen umgesetzt worden. Eingebettete koordinatenbasierte Ortsinformationen waren lange Thema von Privatsphäre-Diskussionen. So gibt es heute einzelne Webdienste, die mit diesen Informationen speziell umgehen. Andere Informationen wie textuelle Ortsinforma-

tionen oder die neueren Personen-Markierungen werden hingegen bisher von keinem Webdienst und keiner Software in Bezug auf das Thema Privatsphäre gewürdigt. Die Schaffung von Bewusstsein über Metadaten muss dafür sorgen, dass die Menschen die Vorteile und Gefahren von Metadaten erkennen und durch die öffentliche Diskussion die Umsetzung weiterer Schutzmechanismen motiviert wird.

4.1.6.3 Komplexität und Nutzbarkeit

Die zuvor beschriebene Vielzahl und Vielfalt von Metainformationen schafft zusammen mit einer stark variierenden Verwendung und Umsetzung in kommerzieller und Open-Source-Software sowie in diversen Webdiensten aus dem einfachen Konzept der Metadaten eine große Herausforderung für die meisten Nutzer. Die geschaffene Komplexität sorgt für Verständnisprobleme bei den Nutzern, aus denen wiederum Bedrohungen der Privatsphäre – häufig durch Unwissen oder schlechte Nutzbarkeit von Software – resultieren können.

Metadaten können heute auf verschiedene Weisen in Bildern gespeichert werden. Die meisten Digitalkameras und mobilen Geräte speichern grundlegende technische Informationen in allen erstellten Bildern. Eine steigende Anzahl von Geräten ermöglicht auch das Speichern von koordinatenbasierten Ortsinformationen. Des Weiteren können Nutzer Metadaten manuell in Bilder integrieren. Dies geschieht über spezielle Metadaten-Software wie beispielsweise *PhotoMe* oder *iExifer*, die ein gewisses technisches Verständnis voraussetzen, sowie über diverse Bildverwaltungsprogramme wie *Adobe Photoshop Elements* oder *digiKam*, die Metadaten in einer proprietären Datenbank ablegen und sie in den Bildern speichern können. Allgemein lässt sich feststellen, dass Programme zur Modifikation von Metadaten bisher quasi nur für Desktop-Systeme existieren, während auf Smartphones oder Tablets vereinzelte Apps nur das Löschen aller Metadaten (wie *Image Privacy* für Android) oder spezieller Metadaten (wie *deGeo* für Apple iOS) erlauben.

Einige Anwendungen unterstützen die Nutzer aktiv bei der Erfassung von Metadaten und ermöglichen eine semi-automatische Annotation. So können Programme wie *Google Picasa*, *Apple iPhoto* oder *Microsoft Windows Live Gallery* auf Basis zuvor markierter Personen Namen zu Gesichtern vorschlagen, um Personen in weiteren Bildern zu markieren. Auf mobilen Geräten erhält diese Technik auch Einzug: Sowohl Apple iOS als auch Android bieten heute grundlegende Unterstützung zum Erkennen von Gesichtern. Bei der Erfassung von Ortsinformationen bieten Anwendungen Funktionen zur Geokodierung, die anhand eines Ortsnamens Koordinaten für ein Bild finden und erfassen. Liegen hingegen Koordinaten vor, so erlaubt die Adresskodierung die Umsetzung dieser in eine textuelle Ortsbeschreibung. Anwendungen auf GPS-fähigen Geräten können beim Teilen im Web den aktuellen Aufenthaltsort als Ort der Aufnahme vorschlagen, wie es beispielsweise die mobilen Apps zu Flickr oder

Facebook tun. Beim Hochladen mit diesen Apps sowie diversen Desktop-Clients werden Teile der eingebetteten Informationen, wie zum Beispiel der Bildtitel, verwendet, um Eingaben für entsprechende Informationen in den Webdiensten vorzuschlagen.

Betrachtet man diese kleine Auswahl von Beispielen, so muss zusammenfassend festgestellt werden, dass es eine Vielzahl von Möglichkeiten gibt, wie Metadaten in Bilder und ins Web gelangen können. Dies stellt eine Herausforderung für die Nutzer dar: Sie müssen den Überblick wahren, welche Informationen letztendlich mit einem Bild weitergegeben werden. Die Nutzer allein müssen in der Lage sein, im Allgemeinen und vor allem beim Teilen von Bildern zu wissen, welche Informationen in ihren Bildern enthalten sind. Die gestaltet sich für viele Nutzer jedoch schwierig.

Möchte sich ein Nutzer selbst gegen Bedrohungen der Privatsphäre durch eingebettete Metadaten schützen, so macht es die große Menge an speicherbaren Metainformationen der verschiedenen Standards sowie das Fehlen einer übergreifenden inhaltlichen Struktur schwierig, die Informationen ausfindig zu machen, die ihn und seine Privatsphäre betreffen könnten. Hinzu kommt, dass die existierenden Softwarelösungen zur Betrachtung und Bearbeitung von Metadaten, so stark voneinander abweichen, dass es für den Nutzer schwierig zu entscheiden ist, ob eine gewählte Software alle für ihn wichtigen Informationen unterstützt oder ob relevante Metadaten nicht visualisiert unerkannt in Bildern verbleiben.

Lediglich wenige Kommandozeilen-Programme wie *Exiv2* oder *Exiftool* zeigen einen Großteil der möglichen Metadaten der verbreiteten Standards an. Diese setzen jedoch auch ein hohes technisches Wissen für die Bedienung voraus. Die mächtigen Werkzeuge scheitern hingegen an der Visualisierung von nicht-textuellen Metadaten, wie Koordinaten oder Markierungen in einem Bild.

Neben der Speicherung in Bilddateien werden Metadaten auf verschiedene andere Weisen gespeichert. Sie können in zusätzlichen Sidecar-Dateien neben einer Bilddatei gespeichert werden, um das Originalbild nicht zu verändern oder Informationen zu speichern, die ein Bildformat nicht unterstützt. Die meisten Bildverwaltungsprogramme speichern Metadaten in einer eigenen Datenbank. Wird ein Foto angezeigt, so werden die separat gespeicherten Metadaten gemeinsam visualisiert. Für den Laien ist es schwer ersichtlich, ob Informationen in den Dateien oder einer Datenbank gespeichert sind und erst recht, wie neu hinzugefügte Metadaten gespeichert werden. Die verschiedenen Möglichkeiten der Speicherung machen es für Nutzer nicht immer einfach den Überblick zu behalten. Erst bei genauerer Beschäftigung mit einigen Anwendungen erfahren sie beispielsweise, dass sie die in einer Datei oder in einer Datenbank gespeicherten Informationen manuell in beide Richtungen synchronisieren können, dies jedoch nicht von allein geschieht. Das fehlende Wissen, wie Metadaten gespeichert sind, macht es schwierig sich im Klaren zu sein, welche verschiedenen Bedrohungen für die Privatsphäre im Einzelnen existieren könnten und

vor allem wie wahrscheinlich eine unbeabsichtigte Preisgabe der Daten ist.

Werden Fotos im Web geteilt, so überträgt sich das Problem der Art der Speicherung auch auf dieses. Metadaten können in Bilddateien gespeichert sein ebenso wie in der Datenbank eines Webdienstes. Die zuvor beschriebenen Probleme existieren somit auch im Web. Dazu kommt, dass die heutigen Webdienste ein stark variierendes Verhalten in Bezug auf die Speicherung beziehungsweise die Erhaltung von eingebetteten Metadaten realisieren. Viele Dienste extrahieren Teile der integrierten Metadaten und speichern sie in ihrer Datenbank. Einige Dienste löschen daraufhin alle integrierten Metadaten aus den Dateien, andere erhalten sie komplett und wiederum andere löschen sie nur teilweise. Dies macht es für die Nutzer quasi unmöglich zu wissen, was in ihren Dateien verbleibt, solange sie es nicht selbst ausprobieren – wozu vielen jedoch das technische Know-how fehlt.

4.2 Bedrohung durch Standortinformationen

Die Preisgabe von Standortinformationen einer Person kann die Grundlage für eine Vielzahl von Bedrohungen ihrer Privatsphäre darstellen. Zudem können aufgrund des starken Bezugs zum Alltagsleben auch Bedrohungen für das Hab und Gut oder sogar das leibliche Wohl betroffener Personen entstehen. Eine betroffene Person ist in diesem Kontext eine Person, die mit gegebenen Standortinformationen in Verbindung gebracht werden kann, so dass Schlüsse über die Person und ihren Ort gezogen werden können. Schlüsse über einen Ort zu ziehen wird dabei heute jedermann durch Dienste wie *Google Maps* oder *OpenStreetMap* ermöglicht, da diese Nutzern erlauben festzustellen, was sich an einem Ort befindet, der durch eine Adresse oder durch Koordinaten beschrieben wird.

Im einfachsten Fall einer Bedrohung der Privatsphäre erfährt jemand, dass eine betroffene Person sich an einem bestimmten Ort aufgehalten hat oder wo diese wohnt, weil diese es selbst im Web veröffentlicht hat. Die Veröffentlichung geschieht zum Beispiel in Form von Metadaten von Bildern [96] oder Nachrichten oder durch Check-ins bei standortbezogenen Diensten. Durch das Aggregieren oder kontinuierliche Aufzeichnen von Ortsinformationen entstehen darüber hinaus diverse Überwachungsszenarien, in denen beispielsweise Hersteller mobiler Betriebssysteme wie *Apple* und *Google* [43] oder Anbieter und autorisierte Nutzer standortbezogener Dienste wie *Foursquare* oder *Facebook Orte* die Bewegungen von Nutzern verfolgen können. Dabei ist zu beachten, dass selbst wenn kontinuierliche Aufzeichnungen anonymisiert werden, Nutzer anhand von Bewegungsprofilen wiedererkannt werden können [128, 137]. Auch wenn man einem Anbieter heute keine bösen Absichten unterstellen möchte, so ist es fraglich, wie dieser in der Zukunft mit den gesammelten Ortsinformationen umgeht. Zudem teilen viele Nutzer ihren Aufenthaltsort mit

Anbietern, die sie selbst nicht identifizieren können: Nutzt jemand beispielsweise eine kostenlose App auf einem mobilen Gerät, welche sich über Werbung finanziert und der der Zugriff auf Ortsinformationen gewährt wurde, so erfahren eventuell auch Werbeanbieter den aktuellen Aufenthaltsort des Nutzers. Dies bemerkt der Nutzer unter Umständen nur, da eingeblendete Werbeanzeigen sich auf die Region beziehen, in der er sich gerade aufhält, oder sich die Sprache der Werbung an sein Aufenthaltsland anpasst. Wie die Preisgabe von Ortsinformationen auch Schaden für das Hab und Gut von betroffenen verursachen könnte, zeigte im Jahr 2010 der Web-2.0-Mashup-Dienst *PleaseRobMe.com*: Verrät eine betroffene Person im Social Web den Ort ihrer Wohnung und später, dass sie vorübergehend nicht zuhause ist, so kann dies zu einer Einladung zu einem Einbruch werden [38]. Die Darstellung dieses realen Problems brachte in Großbritannien sogar Gedanken über die Erhöhung von Hausratsversicherungsbeiträgen für Nutzer von Social Media hervor, wie The Telegraph berichtete [47]. Neben Diebstahl können auch Bedrohungen für das leibliche Wohl oder Menschenleben entstehen, wenn durch die Veröffentlichung von Aufenthaltsorten einer Person der Ort ihrer Wohnung oder regelmäßiger Aufenthalte bekannt wird und sie dort zum Ziel von Stalkern, Kidnappern, Sexualstraftätern oder eines Mörders wird.

4.2.1 Anbieter von Diensten zur Ortsbestimmung

Werden in die Bestimmung des Ortes andere Anbieter einbezogen, wie etwa ein Mobilfunkanbieter oder Dienstanbieter zur WLAN-/mobilfunk-basierten Ortsbestimmung, so darf bei einer Betrachtung der Bedrohung der Privatsphäre nicht außer Acht gelassen werden, dass die Ortsinformationen auch mit diesen geteilt werden. Lediglich Verfahren, die auf Basis externer Signale autark die eigene Position bestimmen, wie es beispielsweise GPS tut, sind von diesem Problem nicht betroffen. Dieser Aspekt sei an dieser Stelle der Vollständigkeit halber genannt. Da im Rahmen dieser Dissertation der Fokus auf der Bedrohung der Privatsphäre durch andere Nutzer und die selbst verschuldete Preisgabe persönlicher Informationen gelegt wird, wird die Bedrohung durch diese Anbieter nicht weiter betrachtet.

4.2.2 Genauigkeit des Ortes

Die Schwere einer Bedrohung durch Ortsinformationen wird durch die Genauigkeit der Informationen beeinflusst. Die Genauigkeit textueller Ortsangaben hängt trivialerweise von der jeweiligen Angabe ab: Die Stadt, der Stadtteil, die Straße oder die genaue Adresse eines Ortes schränken den preisgegebenen Aufenthaltsort einer Person verschieden stark ein. Die Genauigkeit koordinatenbasierter Ortsangaben hängt hingegen in erster Linie von der Technik ab, durch die die Koordinaten ermittelt werden. Die Ortung auf Basis von Mobilfunkzellen ist in der Regel am ungenausten. In

dicht besiedelten Gebieten kann der Ort eines Nutzers auf wenige 100 Meter genau bestimmt werden, indem die Koordinaten des verbundenen Funkmastes ermittelt werden. Genauere Methoden auf Basis von Signallaufzeitmessungen, die zusätzliche Technik aufseiten der Mobilfunkanbieter erfordern, erreichen eine Genauigkeit von bis zu 25 Metern. Die Ortsbestimmung auf Basis eines Globalen Navigationssatellitensystems kann hingegen bis auf wenige Meter genau erfolgen. Hier hängt die Genauigkeit vor allem von der Umgebung ab, die den Empfang der Satellitensignale beeinflusst. Die Genauigkeit der WLAN-basierten Ortung kann nicht exakt spezifiziert werden, da sie zusätzlich zur Umgebung auch von der unbekannt genauen Kartierung von WLAN-Access-Points abhängig ist. Im Stadtgebiet liegt die Genauigkeit häufig unter 50 Metern und zum Teil sogar unter 20 Metern.

Ortsbestimmungen durch den Nutzer geschehen heute in der Regel durch WLAN-basierte Ortung oder die Ortung mittels eines Globalen Navigationssatellitensystems. Die Genauigkeit der preisgegebenen Standortinformationen ist abhängig davon, welche der technischen Verfahren die eingesetzten Geräte bieten, welche von diesen aktiviert sind und wie stark die Beeinflussungen durch Störfaktoren sind, beziehungsweise wie hoch die Dichte kartierter WLAN-Access-Points ist. Es kann nicht genau festgestellt werden, wie genau die durch die Person ermittelten Ortsangaben sind. Jedoch sind sie meist ausreichend genau, um eine deutliche Bedrohung für die Privatsphäre darstellen zu können.

4.2.3 Bewegungsprofile und wiederkehrende Orte

Die Häufigkeit erfasster Standorte bestimmt ebenso die Schwere sowie auch die Art einer Bedrohung. Eine einzelne Ortsangabe sagt lediglich aus, dass eine Person an diesem Ort gewesen ist. Werden mehrere Ortsangaben aufgezeichnet, so entsteht aus diesen ein Bewegungsprofil. Solche Profile können regelmäßige Muster im Verhalten einer Person zeigen und sie so wiedererkennbar oder berechenbar machen. Anhand mehrerer identischer Ortsangaben können Orte identifiziert werden, an denen sich jemand wiederkehrend und daher mit geringerer Wahrscheinlichkeit zufällig aufgehalten hat, was zum Beispiel kombiniert mit Uhrzeiten zu Schlüssen führen kann, wo sich sein Zuhause, seine Arbeitsstätte oder eine beliebte Sportstätte befindet. Ausgehend von solchen Beobachtungen kann spekuliert werden, ob eine Person sich auch in der Zukunft an bestimmten Orten aufhalten wird. Auch lassen sich auf diese Weise Orte identifizieren, deren Bekanntwerden weitere Bedrohungen der Privatsphäre und Schaden verursachen können, beispielsweise wenn sich jemand am Ort bestimmter Fachärzte regelmäßig aufhält.

4.2.4 Anwendungsfälle und Publikum

Abhängig davon, in welcher Art und Weise Ortsinformationen erfasst und preisgegeben werden, entstehen durch das jeweilige Publikum verschiedene Bedrohungen.

Führt jemand mit einem Mobiltelefon ein Gespräch, versendet oder empfängt eine SMS oder nutzt er das Internet unterwegs, so erfasst sein Mobilfunkanbieter seinen aktuellen Aufenthaltsort auf Basis des verwendeten Funkmastes. Durch diese Erfassung erstellen Mobilfunkanbieter implizit Bewegungsprofile eines jeden Nutzers. Wie dies aussehen kann, zeigte im Jahr 2011 der deutsche Politiker Malte Spitz durch die Veröffentlichung von rund 35,000 Ortsangaben, die die Telekom über ihn innerhalb eines halben Jahres gesammelt hatte [55]. Die mögliche Überwachung durch Daten von Mobilfunkanbietern darf nicht unterschätzt werden, jedoch sind diese Informationen im Vergleich zu den folgenden nur einem beschränkten Publikum zugänglich.

Nutzer von Webdiensten, welche aktuelle standortbezogene Informationen zur Verfügung stellen, wie den Ort der nächstgelegenen Autogas-Tankstelle in einer fremden Stadt, teilen ihren aktuellen Aufenthaltsort nur mit dem Dienstanbieter. Somit kann auch nur durch diesen eine Bedrohung entstehen. Da solche Informationen wahrscheinlich nicht all zu häufig oder regelmäßig abgefragt werden, ist die Bedrohung durch diese wohl relativ gering. Deutliche Ausnahmen bilden Dienste zur Abfrage der Wettervorhersage oder auch Dienste zur Abfrage von Verkehrsstaus. Diese werden meist regelmäßiger abgefragt. Jedoch bleibt das Publikum auf den Anbieter beschränkt.

Nutzer von Webdiensten, die der Veröffentlichung des Aufenthaltsortes dienen, teilen ihren aktuellen Aufenthaltsort hingegen mit einem größeren Publikum. Ist die Preisgabe von Ortsinformationen auf ausgewählte andere Nutzer beschränkt, wie die Mitglieder des sozialen Netzwerkes eines Nutzers, so ist das Publikum größer als bei den Informationsdiensten, jedoch klar abgegrenzt für den Nutzer. Hier gelten in etwa dieselben Rahmenbedingungen wie bei den selbstverursachten Bedrohungen durch geteilte Bilder: Das Publikum ist beschränkt, es hat aber eine direkte Verbindung zur betroffenen Person, so dass persönlich motivierte Probleme entstehen könnten. Jedoch kann man dem Nutzer auch unterstellen, dass er nur sehr bedacht ausgewählte Personen auf seinen aktuellen Aufenthaltsort zugreifen lässt. Bekannte Beispiele für Dienste dieser Art sind *Foursquare* oder *Google Latitude*.

Ist die Preisgabe nicht beschränkt und sind die Ortsinformation somit für alle Nutzer eines Dienstes zugänglich oder sogar weltöffentlich, so ist das Publikum entsprechend groß und entsprechend viele Quellen für Bedrohungen existieren. Beispiele für diese Art der Preisgabe von Ortsinformationen sind Ortsangaben von öffentlichen Beiträgen in einer *Facebook*-Chronik, Ortsangaben von *Twitter*-Beiträgen oder Geotags in öffentlich zugänglichen Fotos.

Während die zuvor beschriebenen Dienste einen für den Nutzer deutlichen Ortsbezug haben, gibt es auch Fälle, in denen dem Nutzer nicht klar ist, wann und wofür Ortsinformationen verwendet werden. Dies tritt beispielsweise häufig im Rahmen von Anwendungen auf mobilen Geräten auf und ist äußerst kritisch zu betrachten. Auch die mobilen Betriebssysteme selbst erfassen Ortsinformationen in regelmäßigen Abständen und kartieren so sichtbare WLAN-Access-Points. Google nutzt die erfassten Informationen über den Ort zudem auch, um allen Nutzern eine Anzeige des aktuellen Verkehrsflusses auf Straßen in Google Maps zu ermöglichen. Wofür die Betriebssysteme beziehungsweise die Hersteller die Daten noch verwenden und wer Teil des Publikums ist, ist ebenso unklar wie bei den mobilen Apps.

4.2.4.1 Inhärente Aktualität der Informationen

Abhängig von den verschiedenen Anwendungen sind die preisgegebenen Ortsinformationen eher von historischem Charakter (Ortsinformationen in Fotos oder Blog-Beiträgen), geben den aktuellen Ort des Nutzers an (Check-ins bei einem standortbezogenen Dienst) oder lassen auch Aussagen über zukünftige Aufenthalte zu (Zugriff auf Bewegungshistorie/-profil). Die aus den verschiedenen Anwendungsfällen resultierende Aktualität der Informationen hat auch einen Einfluss darauf, welche Bedrohungen aus einer preisgegebenen Information entstehen können.

4.2.4.2 Mobile Apps

Bedrohungen durch Standortinformationen sind schon seit über 10 Jahren ein Thema der öffentlichen Diskussionen und der Privatsphäre-Forschung [119]. Mit der fortlaufenden Entwicklung standortbezogener Dienste und ihrer wachsenden Nutzerzahl hat sich vermehrt gezeigt, wie wichtig und vielseitig der Schutz von Standortinformationen ist. Jedoch hat erst die immense Nutzung von Ortsinformationen in der Vielzahl von Anwendungen auf mobilen Geräten das wahre Ausmaß der Bedrohung der Privatsphäre in der Realität gezeigt.

Mobile Apps verwenden heute Ortsinformationen wie in allen zuvor beschriebenen Anwendungsfällen. Sie schafften in den letzten Jahren eine Vielzahl neuer standortbezogener Funktionen und Anwendungen. Die meist mit WLAN-Modulen und oft mit GPS-Empfängern ausgerüsteten mobilen Geräte bieten den Nutzern eine einfache Ortsbestimmung und somit eine komfortable Nutzung solcher Apps. Nur eine kleine Auswahl stellen folgende Anwendungsbeispiele dar: die Navigation für Autos, Fußgänger oder Sportboote, das Teilen des eigenen aktuellen Aufenthaltsortes, das Geotaggen von Fotos und Nachrichten, das Beziehen standortbezogener Informationen, der persönliche Lauftrainer mit Routenaufzeichnung und -analyse, die Anzeige von Live-Fahrplänen umliegender Haltestellen von öffentlichen Verkehrsmitteln, das Finden von Mitfahrgelegenheiten und der Erhalt lokaler Rabattcoupons.

Damit eine mobile App die aktuellen Standortinformationen eines Nutzers verwenden darf, muss der Nutzer der App den Zugriff auf diese erlauben. Apple iOS erfragt dazu für jede App, ob diese die notwendige Berechtigung erhalten darf. Verlangt eine Android-App nach der Berechtigung für den Zugriff auf Standortinformationen, wird ihr diese durch die Installation implizit gegeben. Wird der Zugriff auf Standortinformationen nicht durch die zentralen Einstellungen der Systeme unterbunden, können alle Apps mit den entsprechenden Rechten auf die Standortinformationen zugreifen. Dabei kann eine laufende App so oft sie möchte und wann sie möchte auf den aktuellen Aufenthaltsort des Nutzers zugreifen. iOS-Nutzer sehen an einem Symbol in der Statusleiste, wenn Ortsinformationen durch eine App erfasst werden. In den Einstellungen können sie einsehen, ob eine App „kürzlich“ beziehungsweise in den letzten 24 Stunden Ortsinformationen erhalten hat. Android-Nutzer sehen nur ein Status-Icon, wenn der GPS-Empfänger eines Gerätes aktiv ist. Es bietet keinen visuellen Indikator für die Ortung via WLAN und keine Informationen zu vergangenen Ortszugriffen. Die Kontrolle darüber, welche App Ortsinformationen erhalten darf, ist unter Apples Betriebssystem detaillierter. Die Transparenz darüber, welche App Ortsinformationen erhalten hat, ist besser als unter Android, jedoch auch recht gering. Die Nutzer haben keine Übersicht darüber, ob eine App Ortsinformationen nur nutzt, wenn sie dies auch möchten.

Für alle mobilen Geräte ist jedoch ein Faktor, der die Schwere einer Bedrohung der Privatsphäre maßgeblich beeinflusst, identisch: Wird eine Ortsinformation an eine App und damit gegebenenfalls an einen Dienst und den Dienstanbieter preisgegeben, so wird die Ortsinformation in Form von Koordinaten immer mit maximaler Genauigkeit preisgegeben. Selbst wenn ein Nutzer nur eine App verwendet, die ihm das aktuelle Wetter für seine Aufenthaltsregion oder Stadt anzeigt, so wird der App und dem Wetterdienst sein Aufenthaltsort bis auf wenige Meter genau mitgeteilt. Und auch wenn der Nutzer anderen im Web nur mitteilen möchte, das er sich gerade in einer anderen Stadt befindet, und der verwendete Standortdienst nur den Namen der Stadt anzeigt, so teilt der Nutzer dem Dienst zuvor trotzdem seine oft postadressgenaue Position mit. Muss der Nutzer also entscheiden, ob er einer App den Zugriff auf seinen aktuellen Aufenthaltsort gewährt, so steht er immer vor einer Entscheidung von der Art „ganz (genau) oder gar nicht“.

Eine schon zuvor genannte Bedrohung der Privatsphäre bilden solche Apps, bei denen der Nutzer nicht genau weiß, wozu eine App seinen Aufenthaltsort für die von ihm gewünschten Funktionen benötigt. Einige Apps bieten optionale Funktionen an, die auf Ortsinformationen beruhen, die jedoch auch nicht den genauen Aufenthaltsort benötigen würden. So benötigt eine Internetradio-Anwendung nicht den genauen Standort, um Radiosender eines bestimmten Landes bevorzugt anzuzeigen. Hier würde auch die manuelle Auswahl des Landes genügen. Wenn jedoch gar keine

ortsbasierte Funktion zu entdecken ist, ist dies für den Nutzer besonders verwirrend. Dies ist beispielsweise der Fall, wenn kostenfreie Basisversionen von Freemium-Apps mittels Werbung finanziert werden, und die Werbeanbieter diejenigen sind, die den Zugriff auf Standortinformationen fordern. Besonders unter Android ist eine solche In-App-Werbung heute vermehrt zu finden. iOS-Entwickler hingegen generieren ihre Einnahmen zunehmend durch In-App-Käufe.

Kapitel 5

Geteilte Fotos im Social Web

Wie in der Bedrohungsanalyse beschrieben wurde, existieren zwei Formen von Bedrohungen der Privatsphäre durch geteilte Fotos: selbstverursachte und fremdverursachte Bedrohungen. Selbstverursachte Bedrohungen sind oft auf einen falschen Umgang mit Zugriffskontrollmechanismen oder auf unbedachtes Handeln zurückzuführen. Diese Art von Bedrohungen entsteht mehr oder weniger bewusst – die Kontrolle über sie liegt in der Hand des Betroffenen. Selbstverursachte Bedrohungen können vor allem durch Aufklärung und Bildung minimiert werden.

Fremdverursachte Bedrohungen entstehen hingegen durch das Handeln Anderer. Ihre Ursache liegt meist außerhalb des Einflussbereichs eines Betroffenen. Beispielsweise lädt jemand ein Foto hoch, dass die Privatsphäre eines Anderen bedroht. Ist einem Nutzer eine solche Bedrohung bekannt, kann er diese mithilfe des Verursachers oder Dienstanbieters eindämmen, soweit dies technisch und organisatorisch möglich ist. Einer Vielzahl von Bedrohungen dieser Art sind sich die Nutzer jedoch nicht bewusst: Ihnen ist die Bedrohung im Allgemeinen vom Hörensagen her oder aus der Presse bekannt, aber sie wissen nicht, dass oder wo sie betreffende Bilder im Web geteilt werden. Da in diesem Fall weder eine manuelle Suche noch pure Aufmerksamkeit allein Hilfe leisten kann, ist die Suche nach relevanten Fotos eine Herausforderung, der mit technischen Lösungen begegnet werden sollte. Technische Mittel können die Nutzer beim Aufspüren möglicher fremdverursachter Bedrohungen dort unterstützen, wo die manuelle Suche nicht mehr allein zu meistern ist.

Dieses Kapitel befasst sich mit der Untersuchung der fremdverursachten Bedrohungen durch geteilte Bilder, derer sich die Betroffenen nicht bewusst sind.

Überblick Werden Bilder im Web geteilt, so wird die Privatsphäre betroffener Personen durch die Schutzmaßnahmen der jeweiligen Dienste geschützt. Einen grundlegenden Überblick über existierende Schutzmechanismen einer Auswahl häufig verwendeter Social-Media-Dienste gibt Abschnitt 5.1. Die Betrachtung der Dienste zeigt wie komplex und unterschiedlich die Schutzmaßnahmen der Dienste sind. Der Fo-

kus der Betrachtung liegt dabei auf dem Zugriffsschutz und dem Umgang mit Bild-Metadaten. Beim Teilen der Bilder stellt sich neben der Frage nach dem Umgang mit Metadaten auch die Frage danach, wie häufig und welche Metadaten die Nutzer mit ihren Fotos hochladen und teilen. Am Beispiel der Dienste Flickr und Locr beantwortet Abschnitt 5.2 diese Frage. Außerdem wird gezeigt, wie sich die Verwendung von Metadaten über die Zeit verändert hat. Um die Thematik des Bewusstseins über potenziell bedrohliche, geteilte Bilder aus der Sicht der Nutzer genauer zu durchdringen, wurde eine Online-Umfrage zum Bewusstsein über Fotos und Metadaten durchgeführt. Die Ergebnisse der Studie werden in Abschnitt 5.3 präsentiert und diskutiert. Die Studie beleuchtet außerdem das Konzept der Privatsphäre-Kompromisse als Basis für den Schutz privater Informationen. Neben der reinen Existenz von fehlendem Bewusstsein, dass in der Studie deutlich gezeigt wurde, stellt sich ebenfalls die Frage, inwieweit sich die Nutzer über das Ausmaß möglicher Bedrohungen durch Fotos, das heißt, die Menge geteilter Fotos und Metadaten die sie betreffen könnten, bewusst sind. Um dieses zu evaluieren, wurde eine Studie mit Facebook-Nutzern durchgeführt, die ermittelt, wie gut die Nutzer die Dimension möglicher Bedrohungen einschätzen können. Die Studie wird zusammen mit ihren Ergebnissen in Abschnitt 5.4 beschrieben und die Ergebnisse diskutiert. Motiviert durch die Evaluationsergebnisse aktueller Social-Media-Dienste, die Erkenntnisse zum Umgang mit Metadaten durch Dienste und Nutzer und motiviert durch das erfasste Unbewusstsein der Nutzer, werden folgend zwei mögliche Ansätze zur Schaffung von Bewusstsein über Fotos zum Schutz der Privatsphäre präsentiert. In Abschnitt 5.5 werden Konzepte für Dienste vorgestellt, die Nutzer bei der proaktiven Suche nach bedrohlichen Fotos unterstützen können. In Abschnitt 5.6 wird ein insbesondere auf Privatsphäre-Kompromissen basierender Dienst vorgestellt und grundlegend evaluiert, welcher auf Basis von geographischer Kollokation und Gesichtserkennung Nutzer aktiv über potenziell bedrohliche Fotos informieren soll, wenn sie geteilt werden.

5.1 Erhebung über die Privatsphäre in Social-Media-Diensten

Verschiedene Faktoren erschweren den Nutzern den bewussten Umgang mit privatsphärerelevanten Metadaten. Einer dieser Faktoren ist die geringe Transparenz davon, wie Client-Anwendungen und Webdienste mit Metadaten umgehen, welche in Bilder eingebettet sind und mit diesen geteilt werden. Um diese Problematik genauer zu beurteilen, wurde eine Auswahl von Webdiensten untersucht, über die aktuell Fotos geteilt werden. Zusätzlich wurde in diesem Zusammenhang die Verschiedenheit der Privatsphäre-Einstellungen in Form von Zugriffsschutzmechanismen betrachtet. Die ursprüngliche Erhebung wurde Ende 2011 durchgeführt [108]. Die im Folgenden präsentierten Ergebnisse wurden Ende 2013 nochmals verifiziert und aktualisiert.

Flickr Die Foto-Community ermöglicht das Teilen von Fotos in öffentlichen bis hin zu privaten Fotoalben. Von allen betrachteten Diensten bietet Flickr die vielfältigsten Privatsphäre-Einstellungen in Form von Zugriffskontrollen. Durch die vielen Möglichkeiten sind die Einstellungen jedoch auch ebenso schwierig zu überblicken.

Wird ein Foto hochgeladen, so werden die integrierten Metadaten extrahiert und in der Flickr-Datenbank gespeichert. Es werden verkleinerte Versionen des Bildes erzeugt, die keine integrierten Metadaten enthalten. Wird die Originalversion eines Bildes erhalten, so wird sie inklusive aller Metadaten unverändert gespeichert.

Die Privatsphäre-Einstellungen können separat für die Metadaten eines Bildes und das Bild selbst festgelegt werden. So ist es beispielsweise möglich, ein Bild für alle öffentlich im Web zu präsentieren, jedoch den Zugriff auf die Metadaten auf die *Freunde* eines Flickr-Nutzers zu beschränken. Für die Festlegung von Zugriffsrechten stehen folgende Nutzergruppen zur Verfügung: nur der Nutzer selbst, Familie, Freunde, Freunde und Familie, alle Flickr-Nutzer, jeder (öffentlich). Seitdem Flickr-Nutzer die Aktivitäten anderer Nutzer verfolgen können, existiert zusätzlich die Gruppe der Personen, der ein Nutzer folgt. Bei allen Einstellungen ist der meist-öffentliche Zugriff als empfohlene Einstellung gekennzeichnet und oft als Standardwerte voreingestellt. Der Schutz der Privatsphäre wird so als Opt-in-Funktion realisiert.

Für jedes geteilte Bild wird eine der genannten Gruppen als zugriffsberechtigt festgelegt. Das Zugriffsrecht für ein Bild schließt dabei den Zugriff auf die Flickr-eigenen Metadaten-Felder Titel, Beschreibung, Kommentare und Schlagworte (Tags) mit ein, welche über Client-Anwendungen oder die Webseite modifiziert werden können. Beim Hochladen mit vielen Client-Anwendungen und über die Webseite werden einige extrahierte Metadaten wie Schlagworte, Beschreibung und Titel in diesen Feldern gespeichert. Auch manche Felder mit textuellen Ortsangaben (Land, Region, Stadt) werden als Tags gespeichert. Sie sind somit allen zugänglich die auch die Bilder sehen können. Privatsphäre-Einstellungen für die vollständigen, extrahierten Metadaten werden für alle Bilder eines Nutzer zentral und einheitlich festgelegt. Der Nutzer kann festlegen, dass Andere die extrahierten Metadaten nicht sehen dürfen. Des Weiteren kann er speziell den Zugriff auf koordinatenbasierte Ortsangaben der Bilder auf eine der vordefinierten Gruppen beschränken. Den ausgewählten Nutzern werden jedoch nur die extrahierten (oder nachträglich festgelegten) Koordinaten zu den Bildern angezeigt, die der Nutzer zuvor aktiv zu seiner persönlichen Karte hinzugefügt hat. Client-Anwendungen wie die iPhone Flickr-App oder die Instagram-App können dies direkt beim Hochladen tun. Auf der Webseite werden die Koordinaten nur grob auf einer Karte dargestellt. Über die Flickr-API oder den HTML-Quelltext ist der Zugriff auf die genauen Werte jedoch leicht möglich.

Flickr-Nutzern ist es möglich, andere Flickr-Nutzer auf Bildern zu markieren. Optional kann hierbei eine Markierung des entsprechenden Bildbereiches erfolgen.

In der Standardeinstellung können die Kontakte eines Flickr-Nutzers diesen auf Bildern markieren. Die Berechtigung ihn zu markieren kann ein Nutzer alternativ auf eine der beschriebenen Gruppen ändern, wobei alle Flickr-Nutzer anstatt öffentlich die offenste Einstellung darstellt. Für jedes seiner Bilder kann ein Nutzer separat festlegen, ob Personen-Markierungen auf dem Bild generell gestattet sind. Ein besonderes Verhalten zeigt Flickr beim Entfernen der Markierungen: Wenn ein Nutzer eine Markierung seiner selbst auf einem Bild löscht, so kann niemand sonst ihn nochmals auf dem Bild markieren.

Eine weitere Schutzfunktion ist der sogenannte *Geofence*. Er bietet einen zusätzlichen Schutz für koordinatenbasierte Ortsinformationen der extrahierten Metadaten. Die Funktion ermöglicht es Nutzern, private Regionen auf einer Landkarte festzulegen. Liegen Koordinaten von Bildern innerhalb der festgelegten Bereiche, so sind sie für die Öffentlichkeit nicht zugänglich. Ausschließlich für Mitglieder einer der nicht-öffentlichen Gruppen kann der Nutzer den Zugriff dann gewähren. Ist der Zugriff auf ein Originalbild mit integrierten Ortsinformationen möglich, kann jedoch die Geofence-Funktion umgangen werden [21], da diese nicht den Zugriff auf einzelne Originaldateien verhindert, geschweige denn die Originale modifiziert. Abhilfe schafft nur die Möglichkeit, den Zugriff auf Originaldateien generell auf eine der vorgegebenen Gruppen zu beschränken. Die Geofence-Funktion ist als kritisch anzusehen, da sie den Nutzern gegebenenfalls mehr Sicherheit suggeriert als sie wirklich bietet.

Flickr-Nutzer können festlegen, unter welcher Lizenz ein Bild veröffentlicht wird. Die Lizenzwahl hat dabei auch indirekten Einfluss auf die Privatsphäre-Einstellungen: Wird für ein Bild die Creative-Commons-Lizenz gewählt, so setzt dies ein mögliches Zugriffsverbot für die Originaldatei außer Kraft.

Facebook Das Soziale Onlinenetzwerk ermöglicht das Teilen einzelner Fotos im Rahmen der Chronik eines Nutzers oder in Fotoalben. Entsprechend können Zugriffsbeschränkungen für die einzelnen Fotos oder ganze Alben festgelegt werden. Gemäß des sozialen Netzwerkes eines Nutzers können dabei folgenden vordefinierten Zielgruppen gewählt werden: nur der Nutzer selbst, seine Freunde, seine Freunde und Freunde seiner Freunde, Freunde ohne Bekannte oder alle (öffentlich). Zudem können Ausnahmen und eigene Gruppen definiert werden. Der Zugriffsschutz für Bilder kann somit sehr vielfältig umgesetzt werden. Dies birgt jedoch auch die Gefahr von Unübersichtlichkeit oder des Nicht-Ausschöpfens der Funktionalität aufgrund der Komplexität, wenn spontan ein Bild geteilt werden soll.

Alle hochgeladenen Fotos werden verkleinert und dabei die integrierten Metadaten vollständig entfernt[1]. Weder die Originaldateien noch die vollständigen Meta-

[1]Die Verwendung der Browser-Erweiterung aus Kapitel 6 zeigte im April 2014, dass Facebook die eingebetteten IPTC-Angaben zum Ersteller eines Bildes (`Byline`) und zu dessen Urheber (`Copyright`) für Fotos in der Chronik und in Fotoalben aktuell erhielt.

daten werden erhalten. Facebook beschränkt sich somit auf die Metadaten, die in der eigenen Datenbank gespeichert werden. Einige Client-Anwendungen[2] extrahieren beim Hochladen integrierte Metainformationen und füllen damit die Felder Titel und Beschreibung. Neben Titel, Beschreibung und Kommentaren sind in Bezug auf die Privatsphäre vor allem Freitext-Markierungen in Bildern, Personen-Markierungen mit und ohne Markierung im Bild sowie der Ort eines Bildes von Interesse. Diese können über die Webseite, die Facebook-API oder Client-Anwendungen hinzugefügt und verändert werden. Für Metadaten eines Bildes gelten dieselben Zugriffsbeschränkungen wie für ein Bild selbst.

Nutzer können Personen in ihren eigenen Fotos und in denen ihrer Kontakte markieren. Dabei können sie entweder einen Freitext verwenden, oder direkt auf Personen ihres sozialen Netzwerkes verweisen. Verweise können im Bildtitel sowie in Kommentaren als Text erstellt werden. Auf dem Bild selbst kann zusätzlich ein entsprechender Bildbereich markiert werden, dem der Name der Person zugewiesen wird. Für eigene Fotos und Fotos anderer können die Nutzer in den Privatsphäre-Einstellungen festlegen, ob sie erst über Markierungen informiert werden wollen, bevor sie für andere sichtbar werden. So können sie diese moderieren. Die Markierungen beeinflussen auch Zugriffsrechte: Wird eine Person auf einem Bild markiert, kann all ihren Freunden automatisch das Zugriffsrecht auf das Bild eingeräumt werden. Neben dem manuellen Markieren bietet Facebook die Möglichkeit, auf Basis von Gesichtserkennung Markierungen für einen Nutzer vorzuschlagen. Hierzu vergleicht der Dienst Fotos im Freundeskreis mit bisherigen Markierungen eines Nutzers.

Zu Fotos und Alben kann ein Ort festgelegt werden. Als Orte werden dabei durch Nutzer definierte Orte verwendet, die neben Koordinaten auch Namen oder sogar eigene Facebook-Seiten besitzen. Über Client-Anwendungen, wie die mobile Facebook-App, können Nutzer solche Orte erstellen.

Eine hervorzuhebende Bedrohung der Privatsphäre bieten bei Facebook die von Nutzern verwendeten Apps. Die Nutzer teilen auch mit diesen viele ihrer persönlichen Information, um die Apps nutzen zu können. Während dies in der Eigenverantwortung der Nutzer liegt, ermöglichen sie den Apps jedoch oft auch Zugriff auf persönliche Informationen ihrer Kontakte, wenn diese dies durch ihre Privatsphäre-Einstellungen nicht explizit unterbinden.

Viele Schutzfunktionen werden im Rahmen der Privatsphäre-Einstellungen als Opt-in-Funktionen umgesetzt. So kann es passieren, dass neue Funktionen nicht genutzt werden, wenn sie von den Nutzern nicht entdeckt werden. Das Soziale Onlinenetzwerk begründet die Opt-in-Strategie damit, dass einschränkende Privatsphäre-Einstellungen auch den sozialen Charakter des Dienstes einschränken würden.

[2]Die Facebook-Seite selbst extrahierte im April 2014 die IPTC-Angaben `ObjectName`, `Caption` und `Copyright` als Vorgabe für den Titel eines Fotos in Fotoalben.

Picasa Webalben Der Fotodienst ermöglicht das Teilen von Fotos über einen Webbrowser oder aus der Desktop-Software *Picasa* heraus. Der Zugriff auf geteilte Bilder wird pro Album festgelegt. Ein Nutzer hat dabei die Wahl zwischen einem öffentlichen Album, einem Album nur für sich selbst oder einem Album mit Zugriff für all diejenigen, die die geheime Webadresse zum Album kennen.

Wird ein Foto hochgeladen, so werden für die Webdarstellung verkleinerte Versionen der Bilder erstellt, aus denen fast alle integrierten Metadaten entfernt werden. Integrierte Einträge zum Ersteller oder zur eingesetzten Software bleiben beispielsweise erhalten. Picasa Web extrahiert aus den hochgeladenen Bildern die Metadaten und speichert diese wie Flickr in seiner Datenbank. Der Zugriff auf die vollständigen Metadaten ist allen möglich, die Zugriff auf das jeweilige Bild haben. Enthält ein Bild einen eingebetteten Titel, so wird dieser von Picasa Web nach dem Hochladen ausgelesen und übernommen. Der Dienst speichert ein Bild auch im Original, welches heruntergeladen werden kann. Koordinatenbasierte Ortsinformationen genießen einen zusätzlichen Privatsphäreschutz. Für jedes Album kann der Besitzer festlegen, ob Andere Zugriff auf die Ortsangaben bekommen sollen. Wird der Zugriff für ein Webalbum deaktiviert, wird für andere Nutzer in der Webansicht die Kartendarstellung und in der Metadaten-Detailansicht die Ausgabe von Koordinaten unterdrückt. Im Gegensatz zu Flickr schützt diese Funktion auch Koordinaten-Angaben in den gespeicherten Originalbildern: Wird ein Originalbild aus einem Album ohne Zugriffserlaubnis für Ortsangaben heruntergeladen, so erhält ein Betrachter nur eine Kopie des Originals ohne die Ortsangabe. Textuelle Ortsinformationen werden von dieser Schutzfunktion nicht berücksichtigt.

Picasa Web erlaubt das Markieren von Personen mit Namen und der Auswahl eines Bildbereiches. Nur der Besitzer eines Albums selbst kann die Markierungen sehen. Die Markierungen werden in Picasa Webs Datenbank gespeichert und haben keine Auswirkung auf heruntergeladene Originalbilder. Im Vergleich dazu kann die Desktop-Software Picasa solche Markierungen auf Basis des XMP *Metadata Working Group Regions* Schemas in den Bilddateien speichern. Picasa Web ermöglicht eine Zwei-Wege-Synchronisierung von Alben mit der Desktop-Software Picasa inklusive der markierten Personen.

Google+ Das Soziale Onlinenetzwerk integriert Picasa Webalben für die Verwaltung von Fotos. Im Vergleich zu Picasa Web ergeben sich folgende Veränderungen:

Beim Zugriffschutz eines Albums existiert eine weitere Option, mit der der Zugriff auf ein Album für Kontakte oder für *Kreise* eines Nutzers gewährt werden kann. Diese Kontakte können das Album wiederum mit Dritten teilen, wenn es vom Besitzer nicht explizit verboten wird. Nicht nur der Besitzer eines Albums, sondern alle Personen in seinen Kreisen können Personen auf seinen Fotos markieren. Wird ein Nutzer in einem Bild markiert, so kann er sich über die Markierungen informieren

lassen, um diese zu moderieren. Wie bei Flickr kann er auf einem Bild nicht nochmals markiert werden, wenn er es einmal abgelehnt hat. Mit *Find My Face* bietet Google+ eine Funktion, die basierend auf Gesichtserkennung Vorschläge zum Markieren von Personen bietet. Hat ein Nutzer die Funktion aktiviert, so werden ihm und „Personen, die der Nutzer kennt“ Vorschläge gemacht, wenn der Nutzer auf einem Bild erkannt wird.

Windows Live SkyDrive Der Clouddienst ermöglicht das Teilen von einzelnen Bildern oder Verzeichnissen mit Bildern. Die Zugriffskontrolle geschieht über die Weitergabe von Weblinks. Empfänger eines Links können Lese- und auch Schreibrechte erhalten. Außerdem können Fotos öffentlich geteilt werden, so dass sie über die Suchfunktion auch ohne Link gefunden und betrachtet werden können.

Wird ein Bild hochgeladen, so werden kleinere Web-Versionen ohne Metadaten erstellt. Jeder mit Zugriff auf ein Bild hat jedoch auch Zugriff auf die Originaldatei mit allen eingebetteten Informationen. Ein Teil der Metadaten wird bei der Betrachtung eines Bildes dargestellt. Eine Karte visualisiert Koordinaten und Angaben zur Kamera werden angezeigt. Außerdem liest und visualisiert SkyDrive als einziger Dienst Personen-Markierungen aus Dateien, die auf Basis des XMP *Microsoft Photo Region* Schemas gespeichert werden. Diese können beispielsweise mit der Software *Windows Live Fotogalerie* hinzugefügt werden.

Während SkyDrive selbst alle Metadaten in hochgeladenen Bildern erhält, können diese beim Hochladen durch Client-Anwendungen beschränkt werden. *Windows Live Fotogalerie* bietet als Opt-in-Funktion die Möglichkeit alle Metadaten vor dem Hochladen zu entfernen oder selektiv ausgewählte Metadaten, wie zum Beispiel Personen-Markierungen, zu löschen.

Locr Die auf Geotagging fokussierte Foto-Community ermöglicht Nutzern, Bilder mit anderen in Alben organisiert zu teilen. Der Dienst ermöglicht insbesondere auch das Suchen von Bildern über ihren Aufnahmeort. Der Zugriffsschutz wird für jedes hochgeladene Bild einzeln festgelegt. Dazu kann ein Nutzer aus den folgenden Zielgruppen wählen: nur er selbst (privat), Familie, Freunde und öffentlich. Koordinatenbasierte Ortsangaben werden beim Hochladen aus den Bildern ausgelesen und in die Datenbank des Dienstes übernommen. In hochgeladenen Fotos eingebettete Metadaten werden vollständig erhalten. Alle verkleinerten Web-Versionen eines Bildes inklusive der Vorschaubilder enthalten die vollständigen Metadaten. Zugriff auf diese Metadaten hat somit jeder, der auch Zugriff auf ein Bild hat. Weitere Metadaten, wie eine im Web hinzugefügte Überschrift, ein manuell hinzugefügter Ort oder die durch Adresskodierung ermittelten textuellen Ortsinformationen stehen ebenfalls allen mit Zugriff auf ein jeweiliges Bild zur Verfügung.

Apple iCloud Fotostream Der cloudbasierte Dienst ermöglicht Nutzern von iOS und OS X, Bilder zwischen verschiedenen Geräten und mit anderen Personen zu teilen. Werden Bilder über Fotostream geteilt, so werden sie verkleinert und wenig gebräuchliche eingebettete Metadaten teilweise entfernt. Verbreitete Metadaten wie Ortsinformationen oder auch Personen-Markierungen auf Basis des XMP *Metadata Working Group Regions* Schemas bleiben erhalten. Wird ein Bild mit anderen Apple-Nutzern geteilt, wird es mit den verbleibenden Metadaten geteilt. Wird ein Bild über das Versenden eines Weblinks geteilt, so werden die koordinatenbasierten Ortsangaben aus den Metadaten gelöscht, während textuelle Ortsinformationen oder Personen-Markierungen erhalten bleiben und ebenso geteilt werden.

Mobile Apps Verschiedene Apps ermöglichen das Teilen von Fotos bei diversen Webdiensten. Dabei handhaben die Apps in Kombination mit verschiedenen Diensten Bild-Metadaten meist verschieden. Folgendes Beispiel soll dies verdeutlichen:

Die *Instagram*-App ermöglicht das Teilen über den eigenen Instagram-Dienst sowie über andere Dienste wie Flickr, Facebook, Dropbox, oder Foursquare. Wird ein Bild über Instagram selbst geteilt, so wird das Bild verkleinert und alle eingebetteten Metadaten werden entfernt. Optionale Ortsinformationen können über die App festgelegt werden. Bei den anderen Diensten werden die Metadaten abhängig vom Dienst gespeichert. Wird beispielsweise ein Bild über die App bei Flickr hochgeladen, werden die eingebetteten Metadata aus dem Bild entfernt, jedoch werden zuvor Titel, Beschreibung und koordinatenbasierte Ortsinformationen aus dem Bild ausgelesen und können als Flickr-eigene Metadaten übernommen werden. Verwendet ein Nutzer im Vergleich die App *Hipstamatic*, so werden die eingebetteten Metadaten vor dem Hochladen nicht entfernt und Flickr geht mit diesen wie beim Hochladen über die Flickr-Webseite um.

Fazit

Metadaten und speziell koordinatenbasierte Ortsinformationen werden auf erschreckend viele verschiedene Weisen gehandhabt. Einige Dienste entfernen alle Metadaten, eventuell um sich selbst vor Problemen zu schützen, die entstehen können, wenn Nutzer persönliche Informationen im Rahmen ihres Angebots ungewollt preisgeben. Dies ist eine einfache Lösung für die Dienstanbieter, jedoch werden so sämtliche hilfreiche Metainformationen auch für den Nutzer gelöscht, der mithilfe dieser seine persönlichen Daten besser überblicken und beherrschen könnte. Andere Dienste erhalten alle – eventuell auch private – Metadaten und erlauben sogar das Suchen auf Basis einiger Metainformationen. Jede Client-Anwendung bietet einen anderen Privatsphäreschutz. Einige bieten dies als Opt-out, andere als Opt-in und wiederum andere haben gar keine Optionen zum Schutz der Privatsphäre oder zur Kontrolle von veröffentlichten Metadaten.

Werden spezielle Privatsphäre-Schutzmaßnahmen für Metadaten von Diensten angeboten, beschränken sich diese meist auf koordinatenbasierte Ortsangaben. Textuelle Ortsangaben werden bisher nicht beachtet. So gibt es Dienste, die GPS-Koordinaten herausfiltern, die jedoch die genaue Postadresse eines Ortes unangetastet lassen. Auch Personen-Markierungen in Form von eingebetteten Metadaten werden von Schutzmaßnahmen nicht beachtet.

Die aktuelle Umsetzung von Diensten und Anwendungen bringt die Nutzer in die missliche Situation, selbst sehr genau verstehen zu müssen, was wann und wo geteilt wird, um die eigene Privatsphäre vor Bedrohungen zu schützen. Um zu erfahren, wie ein Dienst mit ihren Fotos und Metadaten umgeht, bleibt oft nur es selbst auszuprobieren. Nur wenige weitere Analysen [7] haben sich bisher mit diesem Thema befasst. Bei einigen Diensten ändern sich die Schutzmaßnahmen schneller, während andere wenig Veränderungen zeigten, wenn man die hier beschriebenen Dienste vom Stand Ende 2013 mit dem Stand von Ende 2011 [108] vergleicht.

5.2 Erhebung über die Metadaten von im Web geteilten Bildern

Um das Vorhandensein privatsphärerelevanter Metadaten in aktuellen Fotos einzuschätzen, wurden mehrere Datensätze bestehend aus öffentlich verfügbaren Fotos erstellt und untersucht. Die Analyse der Datensätze zeigt, wie ausgeprägt das Vorkommen von Metadaten in geteilten Bildern aktuell ist. Die erfassten Daten bieten eine Grundlage, um zu beurteilen, inwieweit mögliche Bedrohungen durch Metadaten aktuell bestehen und welche Bedrohungen vorherrschen. Die verschiedenen Datensätze erlauben einen Vergleich klassischer Digitalkameras und mobiler Geräte wie Smartphones und Tablets sowie eine Beurteilung der Veränderung über die Zeit.

5.2.1 Erhobene Datensätze

Es wurden Datensätze für die Onlinedienste Flickr und Locr erhoben.

Der Dienst *Flickr* wurde gewählt, da der Dienst eine der großen und bekannten Foto-Communitys ist, die schon seit den Anfängen des Web 2.0 existiert. Zudem gehört Flickr zu den wenigen Diensten, die zum Zeitpunkt der Erhebungen Foto-Metadaten erhalten haben und sie nicht wie eine Vielzahl anderer löschten. Metadaten finden sich bei Flickr eingebettet in gespeicherten Originaldateien, in Form der von Flickr extrahierten Metadaten[3] und in Form von Flickr-spezifischen Metadaten, die über die Webseite oder über Client-Software/die Flickr-API hinzugefügt werden können. Die öffentliche API erlaubte das legitime Crawlen von Fotos und Meta-

[3] Flickr bezeichnet diese als „Exif-Daten“, extrahiert jedoch auch IPTC- und XMP-Daten

daten. Über sie war der Zugriff auf Informationen zu Fotos und Nutzern möglich. Zusätzlich wurden Webseiten des Dienstes durchsucht: Aus URLs zu persönlichen Foto-Webseiten wurden Nutzernamen und Foto-IDs extrahiert. Auf Basis der Annahme einer gewissen Konstanz der Metadaten-Verwendung eines jeden erfassten Nutzers in Bezug auf das automatische Erfassen durch die jeweilige Kamera und das manuelle Hinzufügen oder Löschen durch den Nutzer wurde genau ein Foto je Nutzer gewählt, um diesen zu charakterisieren.

Der Dienst *Locr* wurde gewählt, um einen Eindruck aktiver Verwendung von Ortsmetadaten zu erlangen. Die Foto-Community ist fokussiert auf Bilder mit koordinatenbasierten Ortsangaben. Zum Zeitpunkt der Datensatzerstellung gehörte Locr zu den Diensten, die Metadaten erhalten haben. Sogar die Vorschaubilder auf der Webseite enthielten die vollständigen Metadaten der Originalbilder. Ergänzend zu den in Bildern eingebetteten Metadaten können Nutzer auf der Community-Webseite den Ort eines Bildes manuell festlegen. Aus den gespeicherten Koordinaten erzeugt der Dienst mittels Adresskodierung textuelle Ortsangaben und zeigt diese im Rahmen der Darstellung der Bilder an. So erlaubt der Dienst einen Einblick in die Nutzung von Adresskodierung. Locr bietet keine öffentliche API zu Fotos oder Metadaten. Daher mussten die auf der Seite hinzugefügten Ortsinformationen aus den Webseiten der Foto-Einzelansichten extrahiert werden. Da das Ziel der Untersuchung der Bilder dieses Dienstes die Beurteilung des Anteils von koordinatenbasierten und textuellen Ortsangaben war und nicht die Erstellung eines repräsentativen Überblicks aller Metadaten, wurden mehrere Bilder pro Nutzer bei der Erfassung zugelassen.

5.2.1.1 Flickr-20k-2011

Der Datensatz *Flickr-20k-2011* wurde im Oktober 2011 erhoben. Er enthält 20.836 Fotos. Zur Erstellung des Datensatzes wurden zuerst Nutzernamen über das Crawlen der Webseite gesammelt. Über die Kalenderfunktion der Seite *Entdecken* → *Interestingness* wurden die ersten fünf Seiten der *Interessanten Bilder* für jeden Tag der Jahre 2009 und 2010, sowie für das Jahr 2011 bis einschließlich des 26. Oktobers durchsucht. Außerdem wurden Nutzernamen durch das wiederholte Durchsuchen der dynamischen Seiten *Entdecken* (neuste geteilte Bilder) und *Entdecken* → *Galerien* (zufällige öffentliche Galerien von Nutzern) gesammelt. Nachdem alle Nutzernamen erfasst worden waren, wurde für jeden Nutzer das bis Ende November 2011 zuletzt hochgeladene Foto heruntergeladen, um repräsentative aktuelle Bilder zu erhalten.

69,5 % der Nutzer in diesem Datensatz hatten eine Pro-Mitgliedschaft von denen 41,6 % den öffentlichen Zugriff auf Originaldateien erlaubten. Für diese 6.021 Nutzer wurde die Originaldatei mit eingebetteten Metadaten heruntergeladen und für die übrigen ein verkleinertes Bild ohne Metadaten. Zu jedem Foto wurden über die Flickr-API – insofern die Zugriffsrechte den öffentlichen Zugriff erlaubten – die von Flickr extrahierten Metadaten bezogen. Der Zugriff auf diese Metadaten wurde

von 22,7 % der erfassten Nutzer nicht erlaubt und weitere 0,9 % der Fotos besaßen keine Metadaten. Des Weiteren wurden für jedes Foto folgende Flickr-spezifische Metadaten gespeichert: Titel, Beschreibung, Schlagworte (Tags), koordinatenbasierter Ort sowie ob Personen (Flickr-Nutzer) auf dem Bild markiert waren.

5.2.1.2 Flickr-3k-mobil-2011

Der Datensatz *Flickr-3k-mobil-2011* wurde ebenfalls im Oktober 2011 erhoben. Er enthält 3.258 Fotos, die maßgeblich mit mobilen Geräten wie Smartphones erstellt wurden. Zur Erstellung des Datensatzes wurden zuerst Nutzernamen auf der Webseite gesammelt. Quelle für Nutzernamen war in diesem Fall die *Kamerasuche*, die nur über die Flickr-Webseite zur Verfügung steht. Nach Kameraherstellern und Modellen geordnet können über diesen Teil der Flickr-Webseite Fotos diverser Kameramodelle betrachten werden. Manuell wurden 33 Kamera-Handys und Smartphones (alle zu diesem Zeitpunkt gelisteten als Smartphone erkennbaren Geräte) ausgewählt. Die neusten Modelle in der Auswahl waren das *Apple iPhone 4S*, das *Samsung Galaxy S2* und das *HTC Desire HD*. Für alle 33 Geräte wurden die Kamerasuche-Webseiten für die Kategorien *Interessante* und *Neueste* wiederholt abgefragt und Nutzernamen extrahiert. Nachdem die Nutzernamen gesammelt worden waren, wurde für jeden Nutzer das bis Ende November 2011 zuletzt hochgeladene Foto heruntergeladen. Dieses Vorgehen führte dazu, dass dieser Datensatz im Vergleich zu den später erhobenen Datensätzen Flickr-50k-mobil-2012/-2013 nicht vollkommen rein mobil ist. Für Nutzer, die sowohl Fotos eines Kamera-Handys als auch Fotos von einer klassischen Digitalkamera hochgeladen haben, wurde mit dem neusten Foto zum Teil unplanmäßig ein nicht-mobiles Foto in den Datensatz aufgenommen. Die klaren Unterschiede der Analyseergebnisse beider Datensätze zeigen jedoch, dass dies nur zu einem geringen Anteil passiert sein kann.

46,7 % der in diesem Datensatz enthaltenen Nutzer hatten eine Pro-Mitgliedschaft und 75,4 % dieser erlaubten den öffentlichen Zugriff auf Originaldateien, so dass für diese 1.148 Nutzer die Originaldatei heruntergeladen wurde. Für die übrigen Nutzer wurde ein verkleinertes Bild gespeichert. Zu jedem Foto wurden die von Flickr extrahierten Metadaten bezogen. Der Zugriff auf diese Metadaten wurde lediglich von 0,1 % der Nutzer des Datensatzes nicht erlaubt und zu weiteren 1 % der Bilder existierten keine Metadaten. Für jedes Foto wurden außerdem folgende Flickr-spezifische Metadaten gespeichert: Titel, Beschreibung, Tags, koordinatenbasierter Ort sowie ob Flickr-Nutzer auf dem Bild markiert waren.

5.2.1.3 Flickr-100k-2012

Der Datensatz *Flickr-100k-2012* wurde Mitte 2012 erhoben. Er enthält 100.710 Fotos. Zur Erstellung dieses Datensatzes wurde Nutzernamen über das Crawlen von

Flickr-Webseiten gesammelt. Über die Kalenderfunktion der Seite *Entdecken* → *Interestingness* wurden die ersten zehn Seiten der Fotosammlungen für jeden Tag von Dezember 2010 bis Juni 2012 auf Nutzernamen hin durchsucht. Weitere Nutzerkennungen wurden durch das wiederholte Abrufen der dynamischen Seiten *Entdecken* → *Interestingness* → *Letzte 7 Tage*, *Entdecken* und *Entdecken* → *Galerien* über die Monate Juni und Juli 2012 hinweg gesammelt. Nach einem Suchdurchgang wurde für jeden neu erfassten Nutzer das zuletzt hochgeladene Foto zusammen mit den Metadaten heruntergeladen.

63,8 % der in diesem Datensatz enthaltenen Nutzer hatten eine Pro-Mitgliedschaft und 64,4 % dieser erlaubten den öffentlichen Zugriff auf Originaldateien. Für diese 41.403 Nutzer wurde die Foto-Originaldatei heruntergeladen. Für die übrigen Nutzer wurde ein verkleinertes Bild gespeichert. Zu jedem Foto wurden die von Flickr extrahierten Metadaten über die API bezogen. 13,2 % der Fotos wurden ohne Metadaten bei Flickr hochgeladen oder die jeweiligen Nutzer erlaubten den Zugriff auf diese nicht. Außerdem wurden für jedes Foto alle Flickr-spezifische Metadaten gespeichert inklusive Titel, Beschreibung, Schlagworte (Tags), Ort (Koordinaten und Text) sowie ob Personen (Flickr-Nutzer) auf dem Bild markiert waren.

5.2.1.4 Flickr-50k-mobil-2012

Der Datensatz *Flickr-50k-mobil-2012* wurde ebenfalls Mitte 2012 erhoben. Er enthält 50.203 Fotos, die mit mobilen Geräten erstellt wurden. Zur Erstellung dieses Datensatzes wurden Paare aus Nutzernamen und Foto-IDs gleichzeitig über das Crawlen der Flickr-Webseite gesammelt. Wurde ein Foto eines noch nicht erfassten Nutzers gefunden, so wurde beides gespeichert. Nach jedem Suchdurchgang wurden die neu erfassten Fotos und ihre Metadaten herunterladen. Auf diese Weise wurde eine Verunreinigung des Datensatzes wie bei Flickr-3k-mobil-2011 verhindert.

Als Quelle für Nutzernamen und Fotos wurde für diesen Datensatz die *Kamerasuche* der Flickr-Webseite verwendet. Manuell wurden 59 Kamera-Handys und Smartphones ausgewählt. Neuere Geräte in der Auswahl waren beispielsweise das *Samsung Galaxy Nexus*, das *Motorola Razr* und das *Nokia Lumia 900*. Für alle 59 Geräte wurden die Kamerasuche-Webseiten für die Kategorien *Interessante*, *Neueste*, *Portrait*, *Makro*, *Nacht* und *Landschaft* kontinuierlich vom 1. Juli bis 17. Juli abgefragt und Nutzernamen und Foto-IDs extrahiert.

37,6 % der in diesem Datensatz enthaltenen Nutzer hatten eine Pro-Mitgliedschaft und 80,4 % dieser erlaubten den öffentlichen Zugriff auf Originaldateien, so dass für diese 15.191 Nutzer die Originaldatei des Fotos heruntergeladen wurde. Für die Übrigen wurde ein verkleinertes Bild gespeichert. Zu jedem Foto wurden die von Flickr extrahierten Metadaten bezogen. 0,4 ‰ der Fotos wurden ohne Metadaten hochgeladen oder die jeweiligen Nutzer erlaubten den Zugriff nicht. Für jedes Foto wurden

zudem alle Flickr-spezifische Metadaten gespeichert inklusive Titel, Beschreibung, Tags, Ort (Koordinaten und Text) sowie ob Flickr-Nutzer im Bild markiert waren.

5.2.1.5 Flickr-50k-mobil-2013

Der Datensatz *Flickr-50k-mobil-2013* wurde Ende 2013 erhoben. Er enthält 54.086 Fotos. Dieser Datensatz wurde auf identische Weise wie Flickr-50k-mobil-2012 erstellt. Nutzernamen und Foto-IDs wurden über die *Kamerasuche* der Flickr-Webseite gesammelt. Dazu wurde die Auswahl der Kameras auf 76 vorwiegend Smartphones erweitert. Die neusten Gerätemodelle waren das *Samsung Galaxy S3 / S4*, das *HTC One* und das *Apple iPhone 5 / 5S*. Einige aktuelle Modelle, wie das *LG Nexus 4* oder das *Samsung Galaxy S3 mini / S4 mini*, konnten nicht erfasst werden, da jede neue Kamera von Flickr manuell in die Kamerasuche integriert wird und diese zu Zeitpunkt der Datensammlung nicht in die Suche aufgenommen worden waren. Um vorwiegend aktuelle Fotos zu sammeln, wurden für die ausgewählten 76 Geräte die Kamerasuche-Webseiten nur für die Kategorie *Neueste* im Zeitraum vom 24. Oktober bis zum 25. November wiederkehrend abgefragt und Namen und Foto-IDs extrahiert. Da dieser Datensatz ergänzend zu Flickr-50k-mobil-2012 verwendet werden sollte, wurden zu jenem doppelt auftretende Nutzer inklusive Foto entfernt.

23,2 % der in diesem Datensatz enthaltenen Nutzer hatten eine Pro-Mitgliedschaft. 91,3 % der Nutzer erlaubten den öffentlichen Zugriff auf Originaldateien, so dass für diese 49.360 Nutzer die Originaldatei des Fotos heruntergeladen wurde. Für die übrigen Nutzer wurde ein verkleinertes Bild gespeichert. Da Flickr seit Mai 2013 auch für Nutzer der kostenlosen Accounts die Originaldateien erhält, ist es korrekt, dass der Anteil der Originaldateien größer als der der Pro-Mitglieder sein kann und ist. Die 8,7 % der Nutzer/Fotos, zu denen keine Originaldatei zur Verfügung stand, müssen den Zugriff entsprechend eingeschränkt haben. Zu jedem Foto wurden die extrahierten Metadaten bezogen. 0,4 % der Fotos wurden ohne Metadaten bei Flickr hochgeladen oder die jeweiligen Nutzer erlaubten den Zugriff nicht. Für jedes Foto wurden zudem alle Flickr-spezifische Metadaten gespeichert inklusive Titel, Beschreibung, Tags, Ort (Koordinaten und Text) sowie ob Flickr-Nutzer auf dem Bild markiert waren.

5.2.1.6 Differenzierung der Flickr-Datensätze

Um Unterschiede zwischen den Datensätzen feststellen zu können, muss gewährleistet sein, dass sich diese ausreichend unterscheiden. Tabelle 5.1 zeigt einen Vergleich der enthaltenen Nutzer und Bilder. Während innerhalb eines Datensatzes ein Nutzer nur einmal enthalten ist, gibt es eine gewisse Überdeckung zwischen den Datensätzen. Ein Teil der mobilen Nutzer ist auch in den allgemeinen Datensätzen enthalten: 3,9 % in den Datensätzen aus 2011 und 12 % in den Datensätzen aus 2012. Bei den

Fotos ist die Überdeckung geringer: 3,5 % in 2011 und 0,6 % in 2012. Vergleicht man alle Datensätze miteinander, so ist die Zahl der Unikate besonders bei den Nutzern in den Datensätzen aus 2011 gering. Das Vorgehen der Datenerfassung hat dies bedingt: Die größeren Datensätze aus 2012 sind von vornherein als Obermenge konzipiert worden. Die Zahl der Unikate ist bei den Fotos weitaus höher (> 95 %), da hier immer neueste Bilder ausgewählt wurden. Die Überdeckung ist für die im Folgenden dargelegten Auswertungen nicht schädlich. Da sie jedoch bekannt sein sollte, wird sie in Form der Unikate je Datensatz in Tabelle 5.1 aufgeführt. Die Tabelle gibt außerdem einen Überblick über weitere Parameter der Datensätze: die Zahl der erfassten Bilder, die Anteile von Pro-Nutzern und erfasster Originaldateien, sowie den Anteil der Bilder, für den integrierte oder extrahierte Metadaten verfügbar waren. Letzterer gibt die Teilmenge der Fotos an, zu denen Metadaten vollständig vorlagen, wie sie die Nutzer hochgeladen hatten.

Jahr /	2011		2012		2013
Datensatz	20k	3k-mobil	100k	50k-mobil	50k-mobil
Nutzer / Fotos	20.836	3.258	100.710	50.203	54.086
Pro-Nutzer	69,5 %	46,7 %	63,8 %	37,6 %	23,2 %
Originaldateien	28,9 %	35,2 %	41,1 %	30,2 %	91,3 %
integr. & extrah. Md.	81,4 %	99,9 %	90,8 %	99,9 %	99,9 %
innerhalb Jahr					
unikale Fotos	99,5 %	96,5 %	99,7 %	99,4 %	*100 %
unikale Nutzer	99,4 %	96,1 %	94,0 %	88,1 %	*100 %
alle Datensätze					
unikale Fotos	97,7 %	96,1 %	99,3 %	99,4 %	100 %
unikale Nutzer	47,2 %	66,3 %	81,4 %	86,8 %	95,9 %

* Vergleich 50k-mobil aus 2012 und 2013

Tabelle 5.1: Differenzierung der Nutzer und Fotos der Flickr-Datensätze

5.2.1.7 Locr-5k-2011

Der Datensatz *Locr-5k-2011* wurde im Oktober 2011 erstellt. Er enthält 4.992 Fotos. Zur Erstellung des Datensatzes wurden die Locr-Webseiten *Neueste Fotos*, *Höchstbewertete Fotos*, *Zufällige Fotos* sowie *Fotos mit den meisten Kommentaren* durchsucht. Für jedes Foto wurde das verkleinerte Vorschaubild gespeichert, welches zum Zeitpunkt der Datensatzerstellung die vollständigen integrierten Metadaten des Originalbildes enthielt. Außerdem wurde zu jedem Foto die Webseite zur Einzelansicht des Bildes gespeichert, um aus diesen die manuell hinzugefügten und textuellen Ortsmetadaten zu extrahieren. Der Datensatz enthält durchschnittlich 2,8 Fotos von 1.771 Nutzern (Median = 1 Foto). Zu 1.122 Nutzer wurde nur ein Foto erfasst, zu 295 Nutzern zwei, zu 121 Nutzern drei und zu 59 Nutzern mehr als 10 Fotos.

5.2.1.8 Locr-25k-2012

Der Datensatz *Locr-25k-2012* wurde im Zeitraum vom 30. Mai bis 27. Juni 2012 erstellt. Er enthält 25.201 Fotos. Die Erstellung des Datensatzes gleicht der des Datensatzes Locr-5k-2011. Der Datensatz enthält durchschnittlich 6 Fotos von 4.135 Nutzern (Median = 1 Foto). Zu 2.327 Nutzer wurde nur ein Foto erfasst, zu 642 Nutzern zwei, zu 321 Nutzern drei und zu 293 Nutzern mehr als 10 Fotos.

5.2.2 Analyse

Im Folgenden werden die Analyseergebnisse der erhobenen Datensätze präsentiert.

5.2.2.1 Klassifizierung privater Metadaten

Zur Analyse der privatsphärerelevanten Metadaten wurden die integrierten und extrahierten Metadaten gemäß der in Listing 5.1 dargestellten Zuordnung klassifiziert. Die erhobenen Flickr-spezifischen Metadaten wurden ebenfalls in diese Klassen eingeordnet. Das Listing zeigt die betrachteten Informationen mit ihrer Bezeichnung gemäß der Nomenklatur der Software/Bibliothek Exiv2:

```
<Standard>.<Namespace|Maker-Note-Format>.<Tag>[/<hierarchische-Sub-Tags>]
```

Listing 5.1: Klassifizierung privatsphärerelevanter Metadaten zur Analyse

```
Kamerahersteller ::= Exif.Image.Make .
Kameramodell ::= Exif.Image.Model .
Kamerabesitzer ::=
   Exif.Photo.CameraOwnerName | Exif.Canon.OwnerName .
Eindeutige Kamera-ID ::=
   Exif.Canon.SerialNumber | Exif.Canon.InternalSerialNumber |
   Exif.Fujifilm.SerialNumber | Exif.Sigma.SerialNumber |
   Exif.Nikon3.SerialNO | Exif.Nikon3.SerialNumber |
   Exif.Olympus.SerialNumber2 | Exif.OlympusEq.InternalSerialNumber |
   Exif.OlympusEq.SerialNumber | Exif.Panasonic.InternalSerialNumber |
   Exif.Pentax.SerialNumber | Exif.Photo.BodySerialNumber |
   Exif.Image.CameraSerialNumber | Xmp.aux.SerialNumber |
   Xmp.MicrosoftPhoto.CameraSerialNumber .

Ersteller oder Künstler ::=
   Exif.Image.Artist | Xmp.tiff.Artist | Xmp.xmpDM.artist |
   Iptc.Application2.Byline | Xmp.dc.creator | Xmp.iptcExt.AOCreator |
   Xmp.plus.ImageCreatorName .
Urheberrechtsinhaber ::=
   Exif.Image.Copyright | Xmp.plus.CopyrightOwnerName .

Schlagworte ::=
   Exif.Image.XPKeywords | Iptc.Application2.Keywords |
   Xmp.dc.Subject | Xmp.lr.hierarchicalSubject .
Titel ::=
   Iptc.Application2.Headline | Exif.Image.ImageDescription |
   Exif.Image.XPTitle | Xmp.dc.title | Xmp.photoshop.Headline .
Beschreibung ::=
   Iptc.Application2.Caption | Exif.Photo.UserComment |
```

```
   Exif.Image.UserComment | Xmp.dc.description |
   Xmp.tiff.ImageDescription .

Geographische Breite ::=
   Exif.GPSInfo.GPSLatitude | Xmp.exif.GPSLatitude |
   Exif.GPSInfo.GPSDestLatitude | Xmp.exif.GPSDestLatitude .
Geographische Länge ::=
   Exif.GPSInfo.GPSLongitude | Xmp.exif.GPSLongitude |
   Exif.GPSInfo.GPSDestLongitude | Xmp.exif.GPSDestLongitude .

Land ::=
   Iptc.Application2.CountryCode | Iptc.Application2.CountryName |
   Iptc.Application2.LocationCode | Xmp.photoshop.Country |
   Xmp.iptcExt.CountryCode | Xmp.iptcExt.CountryName |
   Xmp.iptc.CountryCode .
Staat oder Bundesland ::=
   Iptc.Application2.ProvinceState | Xmp.iptcExt.ProvinceState |
   Xmp.photoshop.State .
Stadt ::=
   Iptc.Application2.City | Xmp.iptcExt.City | Xmp.photoshop.City .
Ort der Aufnahme ::=
   Iptc.Application2.SubLocation | Iptc.Application2.LocationName |
   Xmp.iptc.Location | Xmp.iptcExt.SubLocation |
   Xmp.iptcExt.LocationShown | Xmp.iptcExt.LocationCreated |
   Xmp.xmpDM.shotLocation .
Ort unbekannter Genauigkeit ::=
   Exif.Samsung2.LocationName | Exif.Samsung2.LocalLocationName |
   Exif.Pentax.Location .

Personen-Markierung->Markierung ::=
   Xmp.MP.RegionInfo/MPRI:Regions[1]/MPReg:Rectangle |
   Xmp.mwg-rs.Regions/mwg-rs:RegionList[1]/mwg-rs:Area .
Personen-Markierung->Name ::=
   Xmp.MP.RegionInfo/MPRI:Regions[1]/MPReg:PersonDisplayName |
   Xmp.mwg-rs.Regions/mwg-rs:RegionList[1]/mwg-rs:Name .
```

5.2.2.2 Private Metadaten in Flickr-Bildern (2011)

Auf Basis der Klassifizierung wurde im Jahr 2011 die Menge der Metadaten in geteilten Bildern anhand der beiden Flickr-Datensätze Flickr-20k-2011 und Flickr-3k-mobil-2011 betrachtet [108]. Abbildung 5.1 zeigt eine Auswahl der enthaltenen privatsphärerelevanten Informationen. Die zugrunde liegenden Zahlen zu diesen und weiteren Metadaten sind in Anhang B.1 zu finden. Die Grafik und die im Folgenden beschriebenen Werte geben die erfassten Metadaten in Relation zur Gesamtmenge der Bilder der Datensätze wieder. So entsteht ein Überblick zu wie vielen Fotos Metadaten öffentlich verfügbar waren. Für jede Klasse von Metadaten zeigt die Grafik die Häufigkeit des Vorkommens der Metadaten im Datensatz zufälliger Nutzer (links) neben den Metadaten vorwiegend mobiler Nutzer (rechts). Die gestapelten Balken geben disjunkte Teilmengen der Datensätze wieder, in welche die Fotos der Art der Speicherung der vorgefundenen Metainformationen entsprechend wie folgt gruppiert wurden: In die Bilder eingebettete Metadaten wurden zuerst erfasst. Sind

Metainformationen nicht in einer Bilddatei vorgekommen, wurden als Nächstes die Metainformationen berücksichtigt, die Flickr beim Hochladen extrahiert und in seiner Datenbank gespeichert hat. Zuletzt wurden die Metadaten betrachtet, welche die Flickr-Nutzer über die Webseite oder Software zu einem Bild manuell hinzufügt haben. Durch diese Zuordnung werden alle Metadaten in der Art der Speicherung erfasst, in der sie am engsten an ein Bild gekoppelt sind. Je enger die Kopplung ist, desto größer ist die Gefahr, dass Metadaten mit Bildern verbreitet werden.

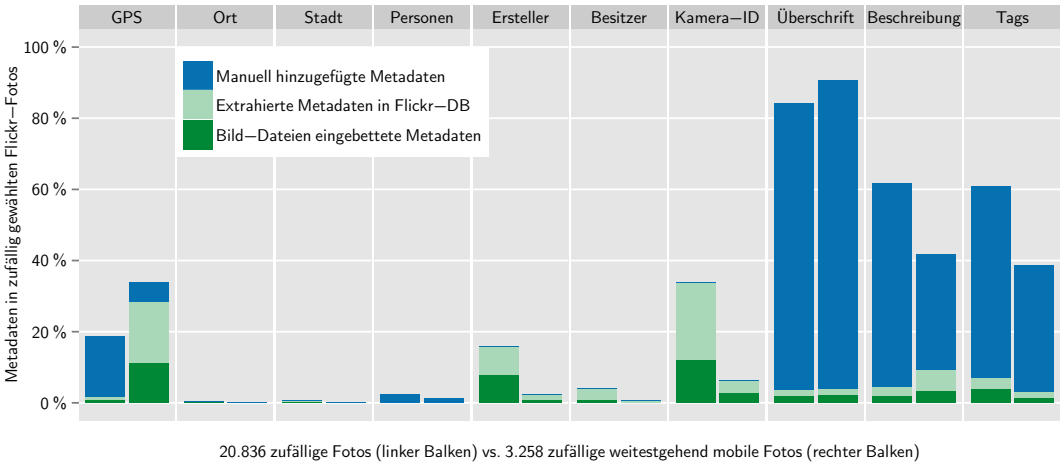


Abbildung 5.1: Privatsphärerelevante Metadaten in öffentlich zugänglichen Flickr-Bildern (2011): 20 k zufällige Bilder im Vergleich zu 3 k weitestgehend mobilen Bildern

Zu 18,7 % der Bilder des Datensatzes Flickr-20k-2011 waren Ortsangaben in Form von Koordinaten verfügbar. Im Vergleich dazu war der Anteil bei den mobilen Bildern des Datensatzes Flickr-3k-mobil-2011 mit 33,9 % beachtlich höher. Zudem macht der Anteil der innerhalb von Flickr hinzugefügten Koordinaten bei den zufälligen Bildern mit 16,9 % (90 % aller Angaben) einen Großteil aus, während er bei den mobilen Bildern mit 5,4 % (16 % aller) weitaus geringer ist. Diese Zahlen zeigen eine klare Tendenz, dass koordinatenbasierte Ortsangaben vorwiegend von mobilen Geräten in Fotos gespeichert werden. Für den Zeitpunkt der Datensammlung war dies nicht verwunderlich, da Smartphones im Gegensatz zu den meisten Kompakt- und Spiegelreflexkameras GPS-Empfänger integrierten und nur wenige Fotografen externe GPS-Logger verwendeten, um ihre Bilder im Nachhinein mit Koordinaten zu versehen. Dieser deutliche Unterschied mag sich in der Zukunft jedoch nivellieren, wenn auch in klassischen Kameras vermehrt GPS-Empfänger verbaut werden.

Textuelle Ortsangaben wie der Aufnahmeort (beispielsweise eine Adresse, ein Stadtteil oder der Name einer Sehenswürdigkeit) und die Stadt sind in den Bildern der beiden Datensätze kaum vorhanden: In den Bildern zufälliger Nutzer sind 0,9 % mit Angaben zum Ort und 1,5 % mit Angaben zur Stadt. In den Bildern der weitestgehend mobilen Nutzer liegen beide Anteile unter 0,5 %. Auch dies mag sich in der Zukunft ändern, wenn Kameras selbst Adresskodierung umsetzen und neben

den Koordinaten eines Ortes auch dessen Namen oder Adresse automatisch in den Bildern speichern. Die Standard-Kamera-App des mobilen Betriebssystems Android tut dies beispielsweise heute schon bei der Anzeige eines Bildes. Sie bettet die Informationen jedoch nicht in neu erzeugte Bilder ein. Welches Ausmaß an textuellen Ortsinformationen eine solche Kodierung heute schon erzeugen könnte, zeigen die Ergebnisse zu den Flickr-Datensätzen aus 2012/2013 sowie die der Locr-Datensätze.

In keinem der Bilder waren Personen-Markierungen gespeichert. Lediglich innerhalb der Flickr-spezifischen Metadaten waren 2,3 % der zufälligen und 1,4 % der mobilen Bilder mit Personen-Markierungen (registrierter Flickr-Nutzern) versehen.

Informationen zum Ersteller eines Bildes (15,7 % der zufälligen; 2,3 % der mobilen), zum Besitzer einer Kamera (4 % der zufällige; 0,6 % der mobilen) sowie die eindeutige Seriennummer/ID einer Kamera (34 % der zufälligen; 6,2 % der mobilen) sind fast ausschließlich in den nicht-mobilen Bildern zu finden. Informationen zum Ersteller werden in der Regel durch Client-Software am PC vor dem Hochladen in Bilder eingetragen. Da vor allem die nicht-mobilen Bilder auf diese Weise geteilt werden, ist der Anteil dort wohl höher. Informationen zum Kamerabesitzer und die Kameraseriennummer werden vorwiegend von einigen klassischen Kameramodellen selbst in die Bilder geschrieben, was den höheren Anteil in den nicht-mobilen Bildern erklärt. Der Anteil der eingebetteten und extrahierten Kamera-IDs ist mit 34 % in Flickr-20k-2011 recht hoch. Das gleichzeitige Vorkommen einer eindeutigen Kamera-ID und des Namens ihres Besitzers erzeugt eine Verknüpfung dieser beiden identifizierenden Informationen, die bei anderen Bildern, welche nur die Kamera-ID enthalten, zum Namen des Besitzers führen könnte. Im Datensatz Flickr-20k-2011 befanden sich zu 3,3 % der Bilder Paare dieser Informationen.

Privatsphärerelevante Informationen können auch in Überschriften, Beschreibungen und Tags zu Bildern gespeichert sein. Wie Abbildung 5.1 zeigt, ist der Anteil dieser Informationen relativ gering in den eingebetteten und extrahierten Metadaten. Hingegen ist der Anteil der in Flickr annotierten Informationen hier sehr hoch. Inwieweit dies für Flickr typisch ist oder allgemein für Foto-Communitys und andere Dienste gültig ist, kann anhand der vorliegenden Daten nicht festgestellt werden.

Beim Betrachten der Metadaten der Datensätze fiel auf, dass in einigen Fällen privatsphärerelevante Metadaten in verschiedenen Feldern wider deren Zweck gespeichert waren. In den Datensätzen befanden sich vereinzelt Telefonnummern, GPS-Koordinaten und verschiedene andere persönliche Informationen als Text in Feldern wie Ersteller, Titel oder Beschreibung.

Hochgeladene Metadaten Die vorherige Auswertung hat gezeigt, zu welchen Anteilen der Fotos beider Datensätze öffentlich zugängliche Metadaten verfügbar waren. Um ferner zu betrachten, wie groß der Anteil an Metadaten ist, die in den Bildern integriert hochgeladen werden, bietet sich eine Teilbetrachtung der Daten-

sätze an. Die integrierten Metadaten der Originaldateien zeigen direkt, mit welchen Metadaten diese Bilder hochgeladen wurden. Die von Flickr extrahierten Metadaten zeigen für einen Teil der übrigen Bilder, welche Metainformationen hochgeladen wurden. Setzt man beide in Relation zur Teilmenge aller Bilder minus die Nicht-Originale ohne Zugriffsberechtigung auf extrahierte Metadaten, erhält man die Anteile der ursprünglich hochgeladenen Metadaten. Abbildung 5.2 visualisiert diese Anteile in Anlehnung an die vorherige Grafik. Eine nicht überprüfbare Einschränkung dieser Vorgehensweise existiert jedoch: Extrahiert Flickr nicht alle enthaltenen Metadaten, so werden diese nicht berücksichtigt. Die ermittelten Anteile könnten somit geringer sein, als sie in der Praxis sind. Nichtsdestotrotz resultieren aus der Analyse nennenswerte Anteile in Form einer unteren Schranke. Betrachtet man beispielsweise koordinatenbasierte Ortsangaben, wird im Rahmen dieser Betrachtung das Ungleichgewicht zwischen den zufälligen und den mobilen Bildern nochmals deutlich: 28,5 % der vorwiegend mobilen Bilder und nur 2,3 % der zufälligen Bilder enthielten demnach beim Hochladen Koordinaten des Aufnahmeortes.

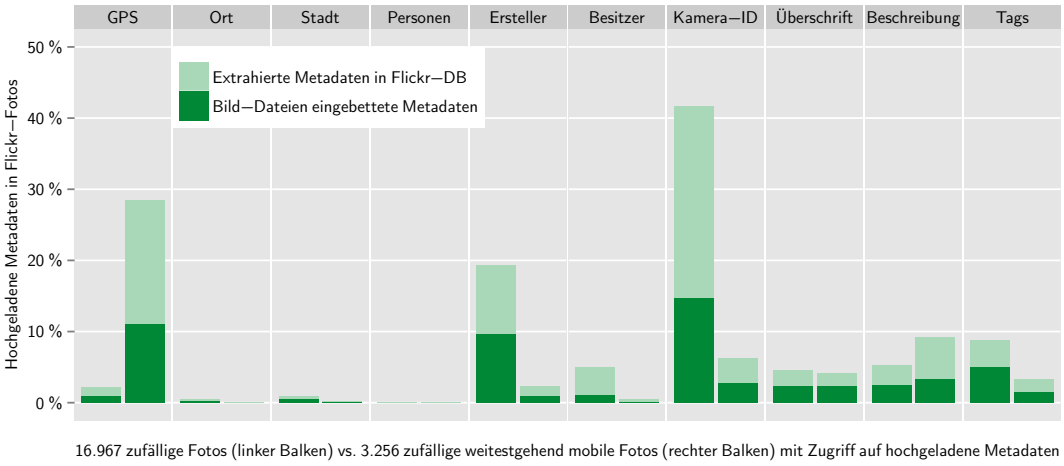


Abbildung 5.2: Mit Flickr-Bildern hochgeladene privatsphärerelevante Metadaten (2011): 17 k zufällige Bilder im Vergleich zu 3 k weitestgehend mobilen öffentlichen Bildern

Fotos mit Georeferenz und nicht-markierten Gesichtern Um die Auswirkungen geteilter Bilder auf andere Personen als die teilenden Personen einzuschätzen, wurden beide Datensätze manuell gesichtet, um den Anteil der Fotos festzustellen, zu denen GPS-Koordinaten vorlagen, jedoch keine Personen-Markierungen. Dies sind diejenigen Fotos, die aufgrund der Bedeutung von Ortsinformationen für die Privatsphäre die Ursache für eine wahrscheinlichere Bedrohung der Privatsphäre abgebildeter Personen werden könnten, welche jedoch aufgrund des Fehlens von Markierungen bei Flickr (wie auch bei Facebook) nicht über diese Bilder informiert werden. Gezählt wurden Gesichter auf Fotos, die komplett in die Kamera schauen, sowie Gesichter im Profil und verdeckte Gesichter, sofern für diese mindestens die Hälfte des Gesichtes erkennbar war. Bilder von Personen auf anderen Bildern, wie

Bilder von Postkarten, Büchern oder Fotos wurden nicht gezählt.

Im Datensatz Flickr-3k-mobil-2011 entsprachen 28,1 % der Bilder den gegebenen Kriterien. Auf den Bildern waren durchschnittlich 2,4 Gesichter zu sehen. Am häufigsten enthielten die Bilder ein einzelnes Gesicht.

In einer zufälligen Stichprobe von 5.000 Fotos des Datensatzes Flickr-20k-2011 entsprachen 17,6 % der Bilder den gegebenen Kriterien. Auf den Bildern waren durchschnittlich 2,2 Gesichter zu sehen. Am häufigsten enthielten die Bilder ebenfalls ein einzelnes Gesicht.

Fazit Flickr hostete lange Zeit Fotos vieler semiprofessioneller Fotografen mit digitalen Spiegelreflexkameras. Schon im Jahr 2011 zeichnete sich ab, dass auch dort mobile Geräte und insbesondere Smartphones die vorherrschende Art von Kamera werden. Schon Ende 2011 war laut Flickrs Kamerasuche-Funktion das Apple iPhone 4S die am häufigsten verwendete Kamera.

Rund ein Drittel der Fotos, die mit diesen vorwiegend genutzten mobilen Kameras erstellt wurden, enthielt koordinatenbasierte Ortsinformationen. Und circa ein Drittel dieser Fotos mit Ortsinformationen zeigte erkennbare Gesichter. Somit können mindestens 10 % der Fotos eine Bedrohung für die Privatsphäre von abgebildeten Personen entstehen lassen.

In den Metadaten wurden Telefonnummern gefunden, jedoch konnte unter diesen Nummern niemand erreicht werden, um eine Stellungnahme zu bekommen. Eingebettete Personen-Markierungen und textuelle Ortsinformationen waren im Jahr 2011 nur in einzelnen Fotos zu finden.

5.2.2.3 Private Metadaten in Locr-Bildern (2011/2012)

Da sich die Foto-Community Locr auf das Thema Geotagging fokussiert, liefert der Dienst einen guten Anhaltspunkt, wie Nutzer, die aktiv an der Verortung von Bildern interessiert sind, dies in der Praxis umsetzen. Um dies zu untersuchen, wurden die Metadaten der zwei Datensätze Locr-5k-2011 und Locr-25k-2012 analysiert. Abbildung 5.3 zeigt die wichtigsten Ergebnisse der Analyse. Die vollständigen Ergebnisse befinden sich in Anhang B.1. Zu fast allen Bildern lagen koordinatenbasierte Ortsinformationen vor. 77,7 % der Fotos des Datensatzes Locr-5k-2011 und 56 % der Fotos des Datensatzes Locr-25k-2012 enthielten eingebettete GPS-Koordinaten. Textuelle Ortsinformationen der verschiedenen Detailstufen waren in 2011 in jeweils circa 6 % der Bilder und in 2012 in jeweils circa 9 % der Bilder eingebettet. Dies ist ein höherer Anteil als bei Flickr, was am Fokus der Online-Community liegen mag. Durch die Adresskodierung des Dienstes waren in 2011 zu weiteren 55 % der Bilder textuelle Ortsinformationen vom Detailgrad Aufnahmeort und Stadt ermittelt worden und in 2012 weitere 60 %. Wie zu erwarten steigt mit gröberen textuellen Ortsangaben

der Anteil an ermittelten textuellen Ortsinformationen: Nicht zu jeder Koordinate lassen sich Straßennamen ermitteln, während die Stadt, die Region oder das Land ermittelt werden können. In naher Zukunft könnte diese Menge an Informationen auch von Kameragerät direkt in die Fotos eingebettet werden.

Der Anteil an eingebetteten Kameraseriennummern fällt in den Locr-Datensätzen auf. Zu 23 % der erfassten Nutzer gibt es eine eindeutige Seriennummer. Zu 6,7 % (2011) beziehungsweise 8,9 % (2012) der erfassten Locr-Nutzer sind in den Bildern eingebettet Paare aus Seriennummer und Kamerabesitzers gespeichert gewesen.

Fazit Der Dienst Locr zeigt exemplarisch, wie mittels Adresskodierung 66 % und mehr der koordinatenbasierten Ortsangaben in textuelle Ortsangaben vom Detailgrad Ort/Straße oder zumindest Stadt umgewandelt werden. Eine automatische Integration dieser Informationen in Fotos würde eine Verstärkung der Bedrohung der Privatsphäre durch Ortsinformationen bewirken. Die Datensätze zeigen auch, dass eine Gefährdung durch Kameraseriennummern existiert: Sie stellen ein weiteres Identifizierungsmerkmal für Nutzer dar.

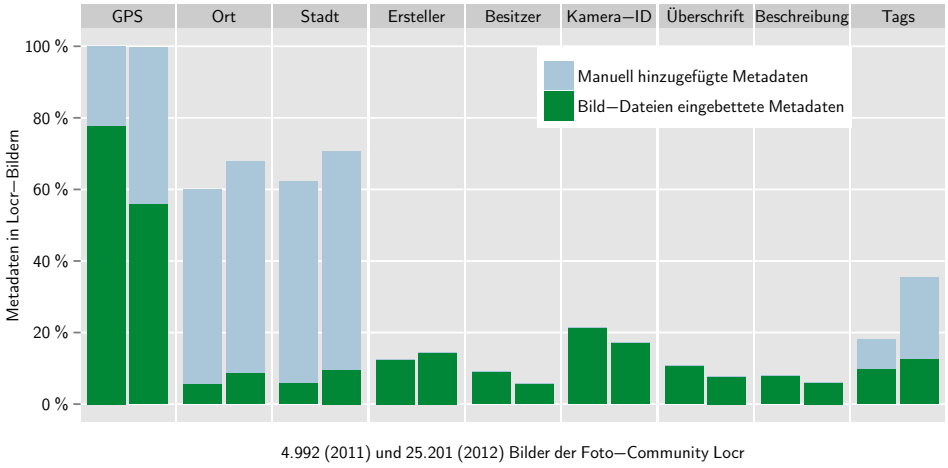


Abbildung 5.3: Privatsphärerelevante Metadaten in öffentlich zugänglichen Bildern der Foto-Community Locr: 5 k Bilder aus 2011 und 25 k Bilder aus 2012

5.2.2.4 Private Metadaten in Flickr-Bildern (2012)

Zur Unterstützung der Analyseergebnisse der Flickr-Datensätze aus dem Jahr 2011 wurden die größeren Datensätze für das Jahr 2012 analysiert. Abbildung 5.4 zeigt eine Auswahl der enthaltenen privatsphärerelevanten Informationen in identischer Darstellung zu den Datensätzen aus 2011. Die Grafik zeigt, zu wie vielen der Fotos Metadaten öffentlich verfügbar waren. In Anhang B.1 befinden sich die vollständigen Metadatenfunde in absoluten Zahlen.

Zur weiteren Betrachtung der Unterschiede werden jene Teildatensätze verglichen, die wie zuvor beschrieben Auskunft über die beim Hochladen integrierten Metadaten

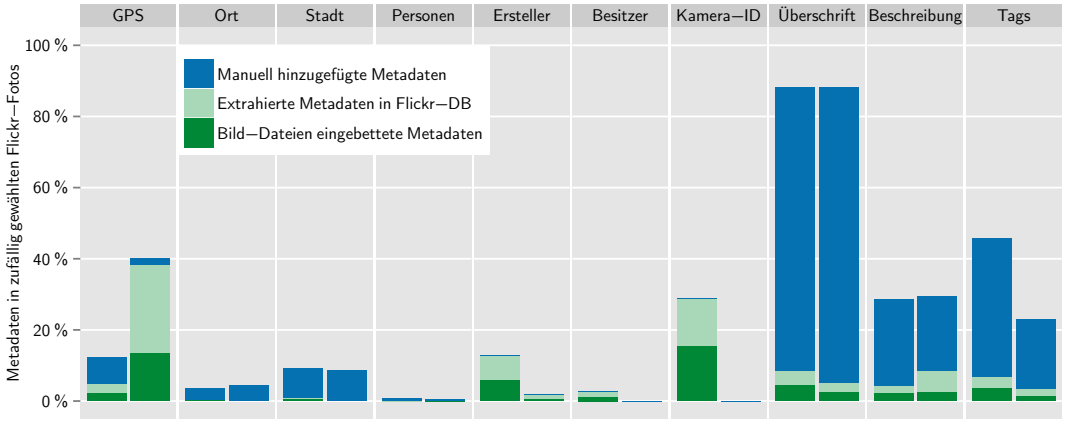


Abbildung 5.4: Privatsphärerelevante Metadaten in öffentlich zugänglichen Flickr-Bildern (2012): 100 k zufällige Bilder im Vergleich zu 50 k mobilen Bildern

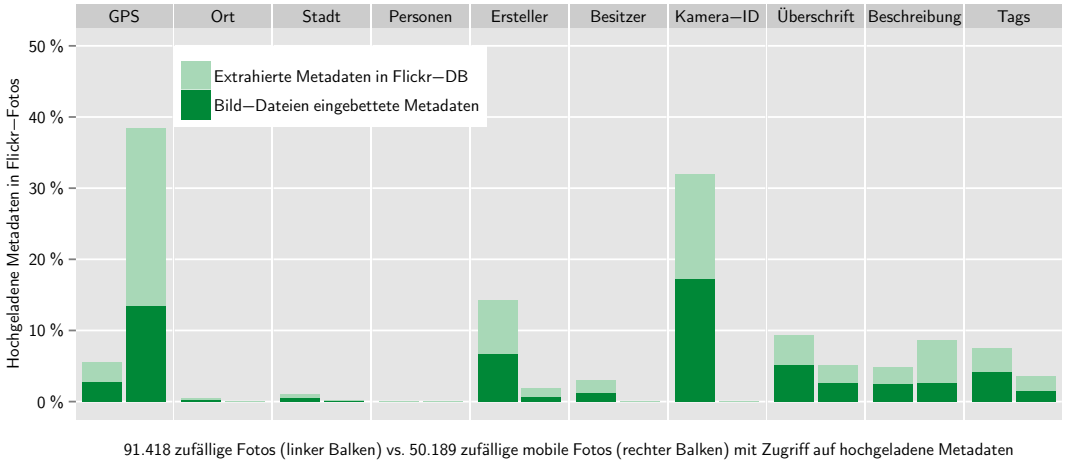


Abbildung 5.5: Mit Flickr-Bildern hochgeladene privatsphärerelevante Metadaten (2012): 91 k zufällige Bilder im Vergleich zu 50 k mobilen öffentlichen Bildern

geben. Abbildung 5.5 stellt die Teilmenge für 2012 analog zur Abbildung 5.2 für 2011 dar. Die im Folgenden beschriebenen Differenzen der Prozentwerte Δ beschreiben die absoluten Unterschiede der Prozentanteile beider Jahre.

Der Anteil von Bildern mit koordinatenbasierten Ortsinformationen ist höher als in den Datensätzen des Vorjahres: Beim Hochladen enthielten 38,4 % der mobilen Bilder ($\Delta = +9{,}9\,\%$) und 5,5 % der zufälligen Bilder ($\Delta = +3{,}3\,\%$) Koordinaten. Der Anteil an textuellen Ortsinformationen vom Detailgrad Stadt und Ort der Aufnahme ist quasi identisch ($\Delta \lesssim +0{,}1\,\%$).

Für die Datensätze aus 2012 wurden auch textuelle Ortsangaben in Form von Flickr-spezifischen Metadaten erhoben. Die in Form von Yahoos *Where On Earth IDs* [69] angegebenen Orte werden aus den Koordinaten generiert. Die durch diese zusätzlich vorhandenen Anteile an Informationen sind jedoch gering im Ver-

gleich zu den ebenfalls durch Adresskodierung gewonnen Informationen in den Locr-Datensätzen: für den Ort der Aufnahme zusätzliche 3,3 % bei den zufälligen Fotos und 4,4 % bei den mobilen, und für die Angabe der Stadt weitere 8,2 % bei den zufälligen Bildern und 8,5 % bei den mobilen.

Die Datensätze zeigen, dass das Einbetten von Personen-Markierungen durch erste Software ermöglicht wird. So treten im Vergleich zu 2011 erstmals Personenangaben nur mit Namen oder auch mit Markierung im Bild auf: Die Anteile befinden sich jedoch noch im Promillebereich (zufällige: $\lesssim$ 0,2‰; mobile: $\lesssim$ 0,3‰). Weitere Personenangaben scheinen im Gegensatz rückläufig. In den zufälligen Bildern sind die Anteile von Ersteller (Δ = -5,1 %), Urheber (Δ = -4,2 %), Kamerabesitzer (Δ = -1,9 %) und Kameraseriennummer (Δ = -9,8 %) gesunken. In den mobilen Bildern ist der Anteil von Ersteller (Δ = -0,4 %) ebenfalls gesunken. Während bei den Inhaltsangaben der Anteil an Überschriften gestiegen ist (zufällige Δ = 4,7 %; mobile Δ = 1,2 %) gibt es bei Beschreibungen und Schlagworten nur geringere Veränderungen.

Fazit Das Vorkommen der integrierten Personen-Markierungen zeigt die Adaption neuer Metadaten-Standards durch Software und Nutzer. Diese stellen eine weitere stark privatsphärerelevante Information in integrierten Metadaten dar. Die Anteile von automatisch eingebetteten Metadaten – allen voran koordinatenbasierten Ortsinformationen – sind gestiegen. Hingegen ist der Anteil manuell hinzugefügter Metadaten leicht rückläufig, eventuell da mehr Bilder von mobilen Geräten aus und gegebenenfalls auch von anteilsmäßig mehr Laien hochgeladen werden. Sollten dies die Gründe für den Rückgang sein, wird verbesserte Software auf mobilen Geräten und Desktop-Systemen den Trend des Rückgangs wahrscheinlich wieder umkehren.

5.2.2.5 Private Metadaten in Flickr-Bildern (2013)

In Bezug auf hochgeladene Metadaten unterscheidet sich der Datensatz Flickr-50k-mobil-2013 nicht erheblich vom mobilen Datensatz aus 2012 (für Details siehe Anhang B.1). Nennenswert ist jedoch der wiederum deutlich gestiegene Anteil der koordinatenbasierten Ortsinformation: Mit einem Anteil von 42,6 % ist er im Vergleich zum Vorjahr nochmals um Δ = +4,2 % gestiegen.

5.2.2.6 Zeitliche Entwicklung der automatischen Metadatenintegration

Die Veränderungen der Anteile der enthaltenen Metadaten über die verschiedenen Datensätze legen nahe, diese in Relation zum Aufnahmezeitpunkt der Bilder betrachten. Aus diesem Grund wurden die Bilder der Datensätze Flickr-100k-2012 sowie Flickr-50k-mobil-2012 und Flickr-50k-mobil-2013 nach Jahren aufgeschlüsselt und die Anteile der Metadaten analysiert. Betrachtet wurde das Vorhandensein öffentlich zugänglicher eingebetteter und durch Flickr extrahierter Metadaten für alle

enthaltenen Fotos. In den mobilen Datensätzen kann dies als korrekte Erhebung aller hochgeladenen Metadaten betrachtet werden, da auf die Metadaten von 99,9 % der Bilder zugegriffen werden konnte. Da dies nur bei 90,8 % der nicht-mobilen Bilder der Fall war, sind die für diese ermittelten Werte als Mindestwerte zu betrachten.

In Bezug auf das Bewusstsein über Metadaten stellen besonders automatisch integrierte Metadaten eine Bedrohung für die Privatsphäre dar. Die vorherigen Analysen zeigten, dass gerade der Anteil dieser Daten eine steigende Tendenz aufweist. Insbesondere die enorme Verbreitung mobiler Geräte ist ein Grund dafür. Aktuell werden vor allem zwei Arten von privatsphärerelevanten Metadaten automatisch durch diese in Bilder integriert. Die Speicherung von koordinatenbasierten Ortsinformationen unterstützen die meisten mobilen Geräte. Außerdem speichern erste Geräte Personen-Markierungen (bisher ohne Namen) in Bildern. Auf diese beiden Informationen konzentrierte sich daher die Analyse.

Die Zuordnung eines Fotos zu einem Jahr geschah für die Analyse wie folgt: Existierte zu einem Foto ein Datum das über einen GPS-Empfänger ermittelt wurde (`Exif.GPSInfo.GPSDateStamp`), so wurde dies verwendet, da Nutzer keinen Einfluss auf dieses haben und es somit als korrekt anzunehmen war. Andernfalls wurde das weiter zurückliegende Datum aus folgenden gewählt: das Datum des Hochladens bei Flickr oder das häufig in Bilder integrierte Erstellungsdatum der Datei (`Exif.Photo.DateTimeOriginal`, sonst `Exif.Photo.DateTimeDigitized`, sonst `Exif.Image.DateTime`).

Tabelle 5.2 zeigt die Ergebnisse der Analyse. Sowohl für die zufällig ausgewählten Nutzer als auch für die mobilen Nutzer zeichnen sich deutliche Trends ab. So stieg der Anteil an Foto mit koordinatenbasierten Ortsangaben in den Fotos zufälliger Nutzer von 1,6 % in 2005 auf 5,1 % in 2012. In den Fotos der mobilen Nutzer stieg der Anteil weitaus stärker 0 in 2006 auf 42,9 % in 2013. In den Bildern der zufälligen Nutzer befanden sich vereinzelt Personen-Markierungen. Ein Trend ist jedoch nicht zu erkennen. Gleiches gilt für Markierungen mit Namen in den mobilen Bildern. Jedoch stieg der Anteil der Personen-Markierungen ohne Namen von 0,15 % in 2011 auf 5,43 % in 2013. Dies erklärt sich damit, dass vor allem Geräte der Firma Apple diese Markierungen seit der Betriebssystem-Version iOS 5 automatisch in Bilder schreiben, so dass in weiterverarbeitender Software nur noch die Namen ergänzt werden müssen.

5.2.2.7 Zusammenfassung

Die Analyse zeichnet ein deutliches Bild vom heutigen Stand der Technik und der vermehrten Nutzung mobiler Geräte als Kameras. Die untersuchten Datensätze enthalten einen zum Teil beachtlichen Anteil an privatsphärerelevanten Metadaten.

Die Fotos der zufällig ausgewählten Flickr-Nutzer enthalten vermehrt solche Metadaten, die manuell hinzugefügt werden. Dies ist damit zu begründen, dass ein noch

	100 k zufällige Nutzer				**100 k Smartphone-Nutzer**			
	Flickr-100k-2012				*Flickr-50k-mobil-2012/-2013*			
Jahr	**Bilder Anzahl**	**Ort [%]**	**Personen [%] Namen**	**BBox**	**Bilder Anzahl**	**Ort [%]**	**Personen [%] Namen**	**BBox**
2005	123	1,6	0	0	-	-	-	-
2006	199	1,5	0	0	60	0	0	0
2007	264	2,7	0	0	227	0,4	0	0
2008	389	2,8	0	0	370	0,3	0	0
2009	637	2,7	0	0	726	24,2	0	0
2010	1.121	2,6	0	0	1.956	38,3	0	0
2011	4.420	4,1	0,05	0,05	5.436	33,7	0	0,15
2012	93.222	5,1	0,01	0,10	48.508	39,3	0,01	1,42
2013	-	-	-	-	49.432	42,9	0,01	5,43

Tabelle 5.2: Anteil an Fotos mit koordinatenbasierten Ortsinformationen und Personen-Markierungen mit Namen oder ohne für 100 k Bilder zufälliger Flickr-Nutzer und für 100 k Flickr-Bilder erstellt mit einem Smartphone oder Kamera-Handy über einen Zeitraum von jeweils 8 Jahren

erheblicher Anteil von Flickr-Nutzern Bilder mit klassischen Digitalkameras aufnimmt und diese über PCs hochlädt, die auch die Möglichkeit bieten über Zusatzsoftware integrierte Metadaten zu modifizieren und zu ergänzen. Die Fotos der mobilen Nutzer enthalten hingegen meist nur Informationen, die automatisch hinzugefügt werden, da diese Fotos wohl oft direkt von den mobilen Geräten aus im Web geteilt werden und diese bisher keine Möglichkeit zur Modifikation bieten, außer alle Metadaten zu löschen. Nur wenige der mobilen Bilder enthalten weitere Informationen, die auf eine Bearbeitung am PC schließen lassen. Dass in der zufälligen Auswahl der Nutzer der Anteil einiger manuell hinzugefügter Metadaten über die Jahre gesunken ist, lässt sich auf den steigenden Anteil an mobilen Kameras zurückführen. Der Anteil der durch diese automatisch hinzugefügten Informationen steigt hingegen.

Die Ergebnisse bestätigen, dass mobile Kamerageräte heute mehr technische Funktionen bieten und so Informationen integrieren, wozu klassische Digitalkameras momentan nicht fähig sind. Dies wird sich in den kommenden Jahren jedoch ändern, wenn klassische Kameras und mobile Geräte weiter verschmelzen.

Koordinatenbasierte Ortsinformationen sind hierfür ein deutliches Beispiel. Die meisten Smartphones integrieren Techniken zur Standortbestimmung und ermöglichen so das Einbetten von Koordinaten in Bilder. Diese Funktion wird auch von einem beachtlichen Teil (bis zu 42,9 %) der Nutzer genutzt und die Koordinaten im Web geteilt. Durch ihre Internet-Anbindung können mobile Geräte ebenso eine Adresskodierung durchführen. Diese wird bisher nur von einem Teil der Geräte bei der Visualisierung verwendet, jedoch nicht beim Erstellen eines Bildes in den Metadaten gespeichert. Dies könnte an einer fehlenden Unterstützung der entsprechenden Metadaten-Standards IPTC und XMP auf den Geräten liegen. Die Ergebnisse zu textuellen Ortsangaben zeigen, wie viel mehr Ortsinformationen durch diese in den

Bildern gespeichert sein könnten. Wird dieses auf den Geräten umgesetzt, kann dies zu einer klaren Steigerung der Bedrohung der Privatsphäre führen, da textuelle Ortsinformationen weniger bekannt sind und auch von Schutzfunktionen bisher nicht berücksichtigt werden.

Das Einbetten von Personen-Markierungen wird momentan von erster Desktop-Software und in einem Teil der mobilen Geräte umgesetzt. Es sind noch keine klaren Trends zu erkennen, jedoch muss beobachtet werden, ob diese Metadaten eine ähnliche Entwicklung wie die lange Zeit kritisch betrachteten Ortsinformationen vollziehen. Zu unterscheiden bleibt dabei, ob nur Gesichter ohne Namen markiert werden, oder ob die Markierungen auf Basis von Gesichtserkennung auch automatisch mit Namen versehen werden. Informationen zu Personen wie der Besitzer einer Kamera oder der Ersteller eines Bildes sind bisher auf nicht-mobile Kameras und das manuelle Hinzufügen beschränkt. Die automatische Integration dieser Informationen durch mobile Geräte wäre einfach umzusetzen. Für das manuelle Hinzufügen jenseits von Desktop-PCs fehlt heute noch ausgereifte Software, so dass mit dem Erscheinen solcher Programme/Apps mit Veränderungen zu rechnen ist.

Die Schwere der Bedrohung durch Freitext-Felder wie Titel, Beschreibung oder Schlagworte wurde nicht vertieft untersucht. Es fielen Einzelfälle auf, jedoch wurde nicht in der Breite evaluiert, wie häufig für die Privatsphäre bedrohliche Informationen in solchen Feldern enthalten sind.

Durch den weiterhin steigenden Anteil an mobilen Geräten und Fotos ist zu erwarten, dass sich die beschriebenen Trends fortsetzen. Ebenso können weitere Informationen automatisiert in Bildern gespeichert werden und ähnlich stark verbreitet werden. Mit dem steigenden Anteil automatisch integrierter Metadaten steigt auch die potenzielle Bedrohung der Privatsphäre durch Metadaten, da besonders durch die automatisch eingefügten Daten unbewusst Informationen verbreitet werden.

5.3 Studie zum Bewusstsein über Fotos im Web

Spätestens seitdem die Medien darüber berichten, dass Arbeitgeber oder Kreditgeber Profilinformationen aus Sozialen Onlinenetzwerken und geteilte Fotos zur Durchleuchtung potenzieller Angestellter oder Kunden verwenden, sind Bedrohungen der Privatsphäre durch im Web geteilte Informationen ein vielerorts diskutiertes Thema. Es ist jedoch fraglich, inwieweit die Öffentlichkeit des Themas bisher dazu führte, dass Nutzer ihr Teil-Verhalten anpassten oder ein generelles Bewusstsein über Bedrohungen durch geteilte Informationen – im Speziellen Fotos – gewachsen ist.

Um die aktuelle Situation zu erfassen, wurde daher eine Studie basierend auf einem Online-Fragebogen durchgeführt [105]. Die Umfrage mit dem Titel „Bewusstsein über Fotos im Internet und die eigene Privatsphäre“ befasste sich mit drei

Teilaspekten: dem Bewusstsein über Fotos, dem Bewusstsein über Foto-Metadaten und den sogenannten Privatsphäre-Kompromissen. Der vollständige Fragebogen ist inklusive der Häufigkeiten der Teilnehmerantworten in Anhang C.1 zu finden.

Diskussion empirischer Daten Für die Analyse der Umfrageergebnisse werden nicht-parametrische Tests verwendet, da Normalitätstests mit dem Kolmogorov-Smirnov-Test statistisch signifikante Abweichungen der Verteilung der Antworten von der Normalverteilung zeigten. Im Folgenden werden Durchschnittswerte der Teilnehmerantworten $\varnothing$ und die dazugehörigen Standardabweichungen s berichtet.

5.3.1 Durchführung

Die Umfrage wurde innerhalb der Leibniz Universität Hannover durchgeführt. Um Teilnehmer für die Umfrage zu rekrutieren, wurden 1.418 Abonnenten eines E-Mail-Verteilers für Studien und Umfragen zu Forschungsthemen angeschrieben. Der Verteilter der Arbeitsgruppe Distributed Computing & Security des Instituts für Verteilte Systeme enthielt vorwiegend E-Mail-Adressen von Studierenden diverser Fachrichtungen und Fachsemester, jedoch auch einen geringen Anteil an Doktoranden und Bediensteten. Über einen Weblink in der Einladung konnten die Eingeladenen direkt an der Umfrage teilnehmen. Um zur Teilnahme an der circa 30-minütigen Umfrage zu motivieren, konnten sich alle Teilnehmer für eine Verlosung zweier Gutscheine für den Online-Shop *Amazon* im Wert von je 50 Euro registrieren.

Eingeladen wurde explizit zu einer Umfrage zum „Teilen (Hochladen) von Fotos, dem Bewusstsein über Fotos im Netz und die eigene Privatsphäre“. Die bewusste Erwähnung des Begriffs der Privatsphäre kann dafür gesorgt haben, dass die Ergebnisse nicht repräsentativ für die betrachtete Zielgruppe sind, jedoch sollten auf diese Weise Nutzer zur Teilnahme bewogen werden, die ein gewisses Interesse am Thema besaßen, um ein Best-Case-Szenario zu erfassen. Für die Verallgemeinerung der Ergebnisse ist wahrscheinlich mit einem schlechteren Ergebnis im Sinne von fehlendem Wissen und Bewusstsein und dem verantwortlichen Handeln zu rechnen. Gleiches gilt für die Übertragung vom universitären Umfeld auf die Population aller Nutzer.

5.3.2 Demographie

Insgesamt wurden 414 vollständige und gültige Beantwortungen des Fragebogens erfasst. 32 weitere wurden als ungültig klassifiziert und zusammen mit 165 unvollständigen Antworten verworfen. 53,9 % der Teilnehmer gaben an männlich zu sein und 46,1 % weiblich. Das Alter der Teilnehmer reichte von 18 bis 43 Jahren mit einem Durchschnitt von 24 ± 3 Jahren. Rund 24,4 % aller Teilnehmer gaben an mindestens einen Universitätsabschluss zu besitzen: Studierende im Zweitstudium oder in einem Master-Studiengang, Doktoranden und Bedienstete waren folglich zu diesem

Anteil vertreten. 22,2 % der Teilnehmer gaben an eine hohe bis sehr hohe technische Expertise zu besitzen.

Die Privatsphäre-Empfindungen der Teilnehmer wurden mittels des Privacy Segmentation Indexes nach Westin wie folgt klassifiziert[4]: 8,2 % der Teilnehmer waren Privatsphäre-Unbekümmerte. 47,8 % der Teilnehmer waren Privatsphäre-Fundamentalisten. Die übrigen 44 % waren Privatsphäre-Pragmatisten. Der Anteil der Unbekümmerten war quasi identisch zu Westins Ergebnissen von Ende 2001 [149]. Der Anteil der Pragmatisten war um 14 % niedriger und der der Fundamentalisten entsprechend höher. Dies mag an den Veränderungen des seitdem vergangenen Jahrzehnts liegen oder auch daran, dass diese Studie in Deutschland durchgeführt wurde. Zusammenfassend lässt sich feststellen, dass sehr viele Teilnehmer an Privatsphäre interessiert waren. Ein Teil ist eher gegen die Preisgabe von Informationen und der andere Teil handelt pragmatisch von der jeweiligen Situation abhängig. Daraus lässt sich folgern, dass die meisten Teilnehmer vermuteterweise an Kontrollmöglichkeiten für persönliche Informationen interessiert sind und dass ihnen das notwendige Bewusstsein über die Verwendung der Informationen dementsprechend wichtig ist.

Die Teilnehmer der Umfrage klassifizierten ihr eigenes Teil-Verhalten wie folgt: Auf die Frage, wie häufig sie Fotos mit anderen im Web teilen, antworteten 49,3 % der Teilnehmer, dass sie Fotos *nie* unterwegs teilen und 10 % gaben an, dass sie Fotos *nie* zuhause über einen PC teilen. Auf der 7-Punkte-Skala von *(1) nie* bis *(7) sehr oft* lag die durchschnittliche Häufigkeit unterwegs bei 2,5 ($s = 1{,}95$) und zuhause bei 3,9 ($s = 1{,}86$). Insgesamt 381 Teilnehmer (92 %) gaben an, Fotos auf die eine oder andere Art im Web zuteilen. Diese 381 Teilnehmer beantworteten die Frage nach der Häufigkeit ihres Teilens wie folgt: 49,9 % der Teilnehmer gaben an, seltener als einmal pro Monat ein Bild im Web zu teilen. 34,4 % antworteten einmal im Monat, 13,4 % einmal pro Woche und 2,3 % einmal oder sogar mehrmals täglich. Diese Angaben lassen vermuten[5], dass die befragten Personen ein eher mittelmäßig ausgeprägtes Teil-Verhalten haben: Sie verweigern sich nicht des Teilens, klassifizierten sich jedoch ebenso nicht als massiv teilende Personen. Auch der Anteil des mobilen Teilens scheint im Gegensatz zum allgemeinen Trend noch recht gering zu sein.

Auf die Multiple-Choice-Frage nach Erfahrungen mit Webdiensten, die das Teilen von Bildern ermöglichen, antworteten die Teilnehmer wie folgt: 85,5 % von ihnen hatten schon einmal Fotos bei Facebook geteilt, 13,8 % bei Google+, 10,1 % hatten Erfahrungen mit Flickr, 7,2 % mit Apple iCloud Fotostream und 3,4 % mit Windows Live SkyDrive.

[4] Die in [105] angegebenen Anteile wurden fehlerhaft berechnet und hier korrigiert.

[5] Es lagen keinen Vergleichszahlen vor, die eine Einordnung der Ausprägung in benannte Verhaltensklassen erlaubt hätte.

5.3.3 Bewusstsein über Fotos im Web

Der erste Teil der Online-Umfrage betrachtete das Bewusstsein der Nutzer über im Web geteilte Fotos, um zu erfassen, inwieweit sich die Nutzer über geteilte Fotos und deren Bedrohungen bewusst sind. Es stellt sich die Frage, ob den Nutzern bewusst ist, dass auch Fotos, die Freunde oder sogar Fremde teilen, eine deutliche Bedrohung für ihre Privatsphäre darstellen. Ebenso stellt sich die Frage, ob die Nutzer ihre Privatsphäre nur von markierten Fotos beeinträchtigt empfinden, oder ob ihnen bewusst ist, dass vor allem auch Bilder ohne Markierung früher oder später zu einer Bedrohung werden können.

5.3.3.1 Personen-Markierungen

Soziale Onlinenetzwerke wie Facebook oder Google+ und Foto-Communitys wie Flickr erlauben ihren Mitgliedern Objekte oder Personen in Bildern zu markieren, so dass eine direkte Verknüpfung zwischen einem Bild und einer Person in Form ihres Online-Pofils entsteht. Diese Markierungen erleichtern es Anderen, Fotos und somit persönliche Informationen über eine Person aufzuspüren, welche zum Teil außerhalb des direkten Einflussbereichs der Person liegen. Auf diese Weise konnten anfangs Informationen preisgegeben werden, die eine Person gegen ihr Einverständnis belasten. Wie schon in der Bedrohungsanalyse beschrieben worden ist, haben diese Markierungen innerhalb kurzer Zeit nach ihrer Einführung eine Menge öffentlicher Kritik geerntet, so dass die Dienstanbieter schnell Möglichkeiten einführten, sich vor dem Bekanntwerden solcher Markierungen über diese informieren zu lassen, um selbst zu entscheiden, welche Markierungen ihrer Person bestehen bleiben und welche nicht veröffentlicht werden. Diese Art von Markierungen hat jedoch auch einen positiven Effekt: Wenn eine Person auf einem Bild markiert wird, so erhält sie eine Benachrichtigung über die Markierung und somit einen Hinweis auf potenzielle Beeinträchtigungen ihrer Privatsphäre. Die Benachrichtigung schafft somit Bewusstsein über ein Bild, von dem die Person eventuell nie oder erst später erfahren hätte. Ein Ziel der Umfrage war, herauszufinden, inwieweit sich die Nutzer über diesen positiven Effekt von Markierungen bewusst sind.

Um zu identifizieren, wieso die Umfrageteilnehmer Personen auf Fotos markieren, wurden sie nach ihren persönlichen Gründen gefragt. Auf Basis der gegebenen 7-Punkte-Skala von *(1) gar nicht* bis *(7) sehr stark* antworteten sie wie in Abbildung 5.6 dargestellt. 30 % der Teilnehmer gaben an, niemals Personen zu markieren, nur um diese über ein Bild zu informieren. Die übrigen 70 % gaben im Durchschnitt eine Antwort vom Wert 5,34 ($s = 1{,}42$), was darauf schließen lässt, dass dies für viele Teilnehmer ein stichhaltiger Grund für das Markieren ist. Im Vergleich dazu gaben 54,8 % der Teilnehmer an, niemals jemanden zu markieren, um Dritte auf ein Foto zu stoßen. Für die übrigen Teilnehmer scheint dies ebenfalls ein geringerer Grund zu

sein, wie ihre durchschnittliche Antwort vom Wert 3,73 ($s = 1{,}55$) vermuten lässt. Die Antworten der Teilnehmer zeigen, dass diese eher Personen markieren, um die Markierten über ein Bild zu informieren, anstatt Dritte auf dies hinzuweisen und ihnen den Zugriff auf das Bild zu ermöglichen.

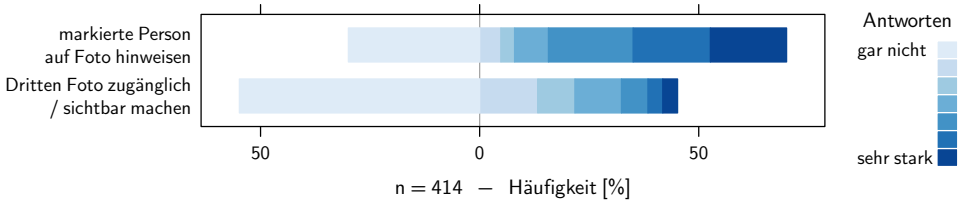


Abbildung 5.6: Gründe für das Markieren von Personen auf Fotos

Um weiterhin zu ermitteln, wie die Teilnehmer es wahrnehmen, wenn sie selbst markiert werden, wurden sie gebeten, das Finden von Fotos durch Markierungen zu bewerten. Die möglichen Antworten lagen dabei auf einer Skala von *(1) gefällt mir sehr* über *(4) neutral* bis zu *(7) stört mich sehr*. Abbildung 5.7 zeigt die Antworten der Teilnehmer. Ihre Antworten zeigen, dass das Bewusstwerden über Fotos ihrer selbst für die Teilnehmer nicht den wichtigsten Effekt darstellt. Vielmehr spiegeln diese den Zeitgeist des Web 2.0 wider: Die Teilnehmer bewerteten, dass sie durch Markierungen Fotos finden können, welche Andere zeigen, mit einem durchschnittlichen Wert von 3,51 ($s = 1{,}37$), derweil sie das Finden von Fotos, welche sie selbst zeigen, mit einem durchschnittlichen Wert von 3,79 ($s = 1{,}8$) bewerteten. Ein Vergleich der Antworten zeigt, dass die leichte Bevorzugung des Findens von Fotos anderer statistisch signifikant ist (Wilcoxon-Test: $z = -3{,}41$, $p = 0{,}001$). Gleichzeitig gaben die Teilnehmer mit einem durchschnittlichen Wert von 4,77 ($s = 1{,}55$) an, dass es sie eher stört, wenn Andere durch Markierungen Fotos finden, welche sie selbst zeigen. Diese Ergebnisse bestätigen eine häufig gemachte Annahme über das Teilen von Fotos im Web: Nutzer finden es gut, auf einfache Weise Fotos von anderen zu finden, während sie es nicht mögen, dass andere ebenso einfach Fotos von ihnen selbst finden. Die Wahrnehmung davon Fotos von sich selbst durch Markierungen zu finden tendiert zur neutralen Antwort. Dies deutet darauf hin, dass die Nutzer einen eher geringen Bewusstsein schaffenden Nutzen in Personen-Markierungen sehen. Die Nutzer markieren Personen eher des Teilens Willen.

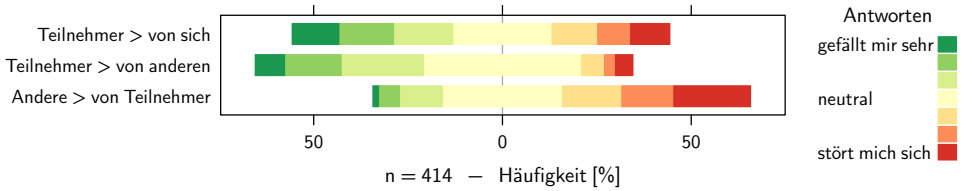


Abbildung 5.7: Wahrnehmung des Effekts von Personen-Markierungen mit Profilverknüpfung: Wer findet Fotos von wem

Schutz begrenzter Reichweite Die positive Wirkung von Personen-Markierungen für den Schutz der Privatsphäre sollte nicht unterschätzt werden. In der Tat sind diese Profilverknüpfungen in den heutigen Sozialen Onlinenetzwerken neben jeglicher Form von aktiver Kommunikation zwischen Teilenden und Betroffenen die einzige Möglichkeit für Nutzer, über Fotos ihrer selbst benachrichtigt zu werden. Die Markierungen bieten ein gewisses Maß an Bewusstsein, jedoch darf nicht vergessen werden, dass dies fast ausschließlich auf die Fotos von Freunden und indirekten Freunden beschränkt ist, da außerhalb dieser Kreise Zugriffskontrollen, fehlende Bekanntschaftsverhältnisse und das Fehlen von Interesse Markierungen verhindern.

Um die Bedeutung dieses Defizits für den Nutzer zu beurteilen, wurde im Rahmen der Umfrage versucht, die Quelle von Bedrohungen der Privatsphäre aus der Sicht der Teilnehmer zu erfassen. Dazu wurden die Teilnehmer gebeten, das Ausmaß einer möglichen Verletzung ihrer Privatsphäre durch Fotos geteilt von verschiedenen Personengruppen einzuschätzen. Die möglichen Antworten lagen dabei auf einer 7-Punkte-Skala von *(1) sehr gering* bis *(7) sehr hoch*. Wie Abbildung 5.8 zeigt, bewerteten die meisten Teilnehmer eine mögliche Verletzung höher als *sehr gering*: Nur 1,4 % aller Teilnehmer bewertete eine mögliche Verletzung durch geteilte Fotos unabhängig von den veröffentlichenden Personen als *sehr gering*. Eine Verletzung durch Fotos von direkten Freunden wurde als am geringsten eingestuft ($\varnothing = 3{,}64$, $s = 1{,}85$). Fotos von indirekten Freunden stellen laut den Teilnehmern eine mittlere Bedrohung dar ($\varnothing = 4{,}69$, $s = 1{,}66$). Fotos, die von Fremden geteilt werden, wurden als größte Ursache für Bedrohungen angesehen ($\varnothing = 5{,}23$, $s = 1{,}95$). Die Unterschiede zwischen den Antworten der Teilnehmer sind statistisch signifikant (Friedman-Test: $\chi^2_2 = 185{,}41$, $p < 0{,}001$; paarweise Wilcoxon-Tests: $z_{1,2} = -10{,}7$, $z_{2,3} = -6{,}4$, $z_{3,1} = -10{,}2$, $p < 0{,}001$). 47 % der Teilnehmer bewerteten eine mögliche Verletzung der Privatsphäre durch Fotos fremder Personen höher als eine durch Fotos von direkten oder indirekten Freunden.

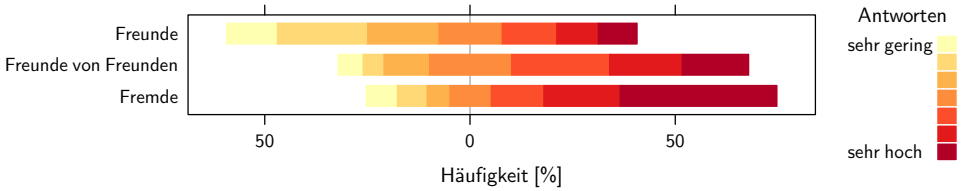


Abbildung 5.8: Einschätzung, wie groß eine mögliche Verletzung der Privatsphäre durch Fotos sein kann, die verschiedene Nutzergruppen teilen

Aus den Antworten lässt sich folgern, dass die Teilnehmer der Umfrage die Bedrohung durch Fotos, die unbekannte Personen teilen, stärker einschätzen als die, welche bekannte Personen verursachen können. Im Gegensatz zu Fotos von direkten und indirekten Freunden und Bekannten werden Fotos, die Fremde teilen, niemals mit Profilverknüpfungen markiert und führen somit auch zu keiner Benachrichtigung.

Somit sind Personen-Markierungen dieser Art – auch dem Gefühl der Nutzer nach – ernstzunehmend defizitär, da sie keine Hilfe bei der Schaffung von Bewusstsein im Falle der am meisten als bedrohlich eingestuften Bilder bieten.

Die Ergebnisse über das Ausmaß möglicher Privatsphäre-Verletzungen legt die Vermutung nahe, dass die Teilnehmer nicht davon ausgehen, dass andere ihrer „moralischen Verpflichtung“[6] nachkommen, und so die Privatsphäre betroffener nicht wahren, obwohl die meisten Teilnehmer selbst erklärten, die Privatsphäre anderer zu achten, wenn sie Bilder teilen. Letzteres zeigte sich, bei der Frage, nach welchen Kriterien die Teilnehmer entscheiden, ob sie ein Foto im Netz teilen oder nicht. Auf Basis der 7-Punkte-Skala von *(1) gar nicht* bis *(7) sehr stark* gaben die Teilnehmer folgende Einschätzungen ab, wie sehr sie einen Schaden für ihre eigene Person und Schaden für andere Personen in die Entscheidung des Teilens einbeziehen. Nur 2 % der Teilnehmer antworteten, dass sie *gar nicht* über mögliche Schäden für andere nachdenken, wenn sie ein Bild im Web teilen. Von den übrigen Teilnehmern bewerteten rund 61 % einen Schaden für andere und Schaden für sich selbst als gleich starkes Kriterium für eine Teil-Entscheidung. 6,6 % der Teilnehmer bewerteten Schaden für andere sogar als ausschlaggebender als Schaden für sich selbst. Dies spricht für ein gewisses moralisches Abwägen bei den Umfrageteilnehmern, während sie dies den Ergebnissen nach anderen Personen nur begrenzt zugestehen.

5.3.3.2 Bewusstsein heute

Im Kontext des Bewusstseins über geteilte Fotos müssen ebenfalls die Fotos betrachtet werden, welche eine Person identifizieren können, die jedoch weder eine Profilverknüpfung besitzen noch zu einer Benachrichtigung führen. Die Identifizierung kann beispielsweise durch Namen in einem Bildtitel, in Kommentaren oder durch eingebettete Bild-Metadaten geschehen. Wie in der Bedrohungsanalyse beschrieben wurde, stellen solche Fotos eine größere Bedrohung als die zuvor betrachteten Bilder dar, da Nutzer nicht informiert werden und eine Bedrohung oft lange im Verborgenen bleiben kann, bevor später eventuell Schaden entsteht. Bisher hilft zum Schutz vor dieser Art von Bildern, genauso wie bei Bildern ohne identifizierende Merkmale bis auf das Motiv selbst, nur eine proaktive Suche. Im Rahmen der Umfrage wurden die Teilnehmer gefragt, wie groß sie das Risiko einschätzen, dass jemand irgendwann ein Foto findet, welches sie zeigt, welches die Person jedoch nicht hätte sehen sollen. Für die zuvor genannten drei Szenarien bestimmten sie das empfundene Risiko auf einer 7-Punkte-Skala von *(1) sehr gering* bis *(7) sehr groß*. Abbildung 5.9 visualisiert die Verteilung der Antworten. Während 24 % der Teilnehmer das Risiko als *sehr ge-*

[6] gemäß „moral obligation“ in [78]: Es ist die Aufgabe des Besitzers/Hochladenden eines Bildes die Privatsphäre abgebildeter Personen zu bewahren.

ring einschätzten, dass zukünftig jemand ungewollt ein Foto findet, das zuvor durch eine Personen-Markierung mit ihrem Profil in einem Onlinedienst verknüpft worden ist, betrachteten nur 11 % das Risiko als *sehr gering*, dass jemand ungewollt ein Foto findet, welches ihren Namen enthält oder sie nur im Motiv zeigt. Dieses Ergebnis ist offensichtlich, da die markierten Personen in der Praxis in der Regel über die entsprechenden Bilder informiert werden und diese entfernen lassen können, wenn sie es möchten. Die Nutzer sehen größere Bedrohungen durch ihnen unbekannte Fotos, die eine Referenz auf ihre Person enthalten, als durch Fotos, die sie lediglich darstellen. Im ersten Fall wählten 45 % der Teilnehmer eine der drei höchsten Bewertungen für das Risiko. Im zweiten Fall taten dies nur 35 %. Der Unterschied dieser Antworten ist statistisch signifikant (McNemar-Test: $\chi^2 = 10{,}32$, $p = 0{,}001$). Dies weist darauf hin, dass die Teilnehmer glauben, dass Fotos mit enthaltenen Referenzen auf Personen einfacher zu entdecken sind, beispielsweise über eine entsprechende Web-Suchmaschine, während die ohne Referenz schwerer zu finden sind. Auch wenn so etwas heute noch nicht in der Praxis umgesetzt ist, schätzen sie dieses dem heutigen Stand der Technik entsprechend korrekt ein.

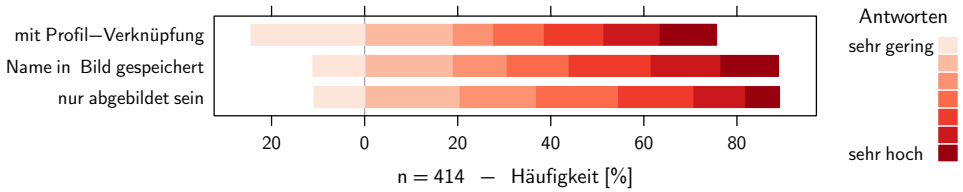


Abbildung 5.9: Einschätzung des Risikos, dass zukünftig jemand ein Foto einer Person findet, in Abhängigkeit verschiedener Referenzen auf die Person

Im Rahmen der Umfrage wurde erfasst, wie die Teilnehmer momentan von Fotos ihrer selbst erfahren und inwieweit sie mit den aktuellen Möglichkeiten zufrieden sind. Um Ersteres zu beurteilen, wurden die Teilnehmer mittels einer Multiple-Choice-Frage gefragt, wie sie momentan von den Fotos erfahren. 75 % der Teilnehmer antworteten auf diese Frage automatisch per E-Mail informiert zu werden, wenn sie in einem Foto markiert werden (94 % dieser Teilnehmer waren Facebook-Nutzer). 52 % der Teilnehmer gaben an, durch Zufall auf entsprechende Fotos aufmerksam zu werden. 39 % von ihnen antworteten, dass sie in Gesprächen von Fotos erfahren. 30 % hingegen in Nachrichten von Freunden. 18 % der Teilnehmer gaben an, aktiv nach Fotos von sich zu suchen. 4,6 % gaben an, dass sie durch Nachrichten von anderen Personen als ihren Freunden von Fotos ihrer selbst erfahren und 3,4 % der Teilnehmer gaben an, gar nicht von Fotos zu erfahren, die sie abbilden. Diese Zahlen geben einen Eindruck, wie stark welches Medium für Bewusstsein sorgt. Jedoch müssen folgende Einschränkungen bedacht werden: Die von drei Vierteln der Teilnehmer genannte automatische Benachrichtigung existiert nur für Fotos, die mit einer Profilverknüpfung innerhalb eines Webdienstes versehen werden. Ferner

sind alle genannten Möglichkeiten sich über Fotos seiner selbst bewusst zu werden auf Fotos im direkten oder maximal indirekten Bekanntenkreis beschränkt und helfen außerhalb dieser nicht. Die Möglichkeit eigene Freitext-Antworten hinzuzufügen zeigte, wie verschieden die Meinungen der Teilnehmer über das Teilen und Betroffensein sind. So schrieben sie beispielsweise „es gibt keine Fotos von mir“, „Fotos werden nur mit meinem Wissen hochgeladen“ und „bin nicht mehr bei Facebook, aber werde immer noch im Netz auf Bildern durch Freunde zu sehen sein“.

Die Teilnehmer wurden außerdem gefragt, wie sehr sie sich über sämtliche Fotos im Web, auf denen sie zu sehen sind, informiert fühlen. Auf der gebotenen 7-Punkte-Skala von *(1) völlig ausreichend* bis *(7) äußerst ungenügend* war das wahrgenommene Informationsniveau im Falle von schönen und angenehmen Fotos im Durchschnitt gering unter dem mittleren Wert von 4, d. h. geringfügig ausreichend ($\varnothing = 3{,}2$, $s = 1{,}85$). Im Falle von nicht gewünschten oder unangenehmen Fotos war die durchschnittliche Wahrnehmung des Informiertseins exakt im mittleren, neutralen Bereich ($\varnothing = 4$, $s = 1{,}85$). 22 % der Teilnehmer gaben an, dass ihr Informationsniveau im Falle der schönen Fotos *völlig ausreichend* sei, während 25 % eine Antwort schlechter als neutral bis zu *völlig ungenügend* wählten. Im Vergleich dazu gaben nur 11 % der Teilnehmer an, dass ihr Informationsniveau im Falle der unerwünschten Fotos *völlig ausreichend* sei, während 39 % eine Antwort schlechter als neutral bis zu *völlig ungenügend* wählten. Die Unterschiede zwischen den zwei Arten von Fotos weisen eine statistische Signifikanz auf (McNemar-Test: $\chi^2 = 50{,}77$, $p < 0{,}001$). Abbildung 5.10 zeigt die genauere Verteilung der Antworten.

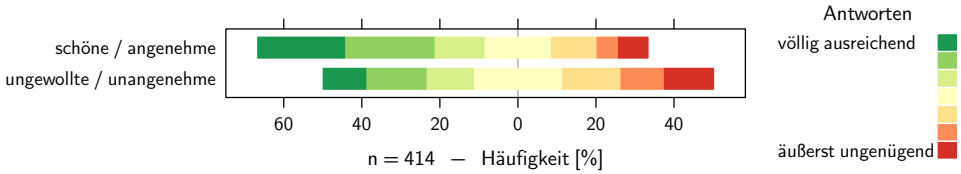


Abbildung 5.10: Wahrgenommenes Informationsniveau über sämtliche Fotos im Web, die die Studienteilnehmer zeigen

Zum Abschluss des Umfrageabschnitts zum Bewusstsein über Fotos im Web wurden die Teilnehmer gefragt, ob sie unter der Annahme, dass es einen Dienst gäbe, der eine Möglichkeit bietet sie über Fotos ihrer selbst zu informieren, auch Zeit investieren würden die gemeldeten Fotos zu sichten. 53,1 % der Teilnehmer antworteten auf diese Frage mit einem klaren Ja. 41,8 % waren an solch einem Dienst interessiert. Nur 3,6 % der Teilnehmer entschieden sich für die Antwort, dass ihnen der Aufwand die Bilder durchzusehen vermutlich zu groß wäre. Die Übrigen verneinten ebenfalls und appellierten an die Moral der Teilenden oder waren der Meinung auf keinen Fotos abgebildet zu sein, wie sie mit ihren Kommentaren zeigten.

5.3.3.3 Zusammenfassung

Die Schaffung von Bewusstsein über im Web geteilte Fotos, auf denen Personen abgebildet sind, ist eine grundlegende Voraussetzung, um Bedrohungen der Privatsphäre durch solche Fotos verhindern zu können. Das Markieren von Personen, das Profilverknüpfungen und Benachrichtigungen der Markierten bewirkt, ist momentan eines der wenigen Mittel von unbekannten Fotos zu erfahren, auf denen eine Person abgebildet ist. Die Teilnehmer der präsentieren Umfrage sahen einen eher geringen Bewusstsein schaffenden Nutzen in solchen Markierungen. Selbst wenn sie diesen Effekt der Markierungen wahrnehmen würden, ist der Nutzen auf Fotos von direkten und indirekten Freunden beschränkt. Fotos, welche von anderen Personen oder außerhalb genutzter Webdienste veröffentlicht werden, profitieren davon nicht. Genau diese Fotos bergen laut der Wahrnehmung der Teilnehmer die größte Bedrohung für die Privatsphäre. Die Teilnehmer zeigten, dass sie das Risiko, dass jemand ein Foto von Ihnen ungewollt findet, im Falle von Fotos mit identifizierenden Merkmalen und ohne Profilverknüpfung oder Fotos ohne jegliche Markierung, am größten einschätzen. Es gibt bisher keine technischen Hilfsmittel, um von solchen Fotos zu erfahren, außer händisch nach diesen zu suchen. Als die Teilnehmer gefragt wurden, auf welchem Wege und wie effektiv sie bisher über Fotos informiert werden, auf denen sie zu sehen sein könnten, bestätigten ihre Antworten, dass technische Lösungen zur Schaffung von Bewusstsein über geteilte Bilder zum Schutz der Privatsphäre benötigt werden. Obwohl andere wissenschaftliche Arbeiten gezeigt haben, dass Nutzer oft wenig Zeit in die Konfiguration von Privatsphäre-Einstellungen investieren, haben fast alle Teilnehmer signalisiert, zumindest in gewissen Maßen Zeit investieren zu wollen und Fotos durchzusehen, wenn Ihnen die Möglichkeit geboten werden würde, über mögliche Bedrohung der Privatsphäre informiert zu werden. Ein Teilnehmer war sogar bereit, eine einmalige Gebühr für solch einen Dienst zu bezahlen.

5.3.4 Bewusstsein über Foto-Metadaten

Bis dato wurden nur wenige Metadaten in Bezug auf die Privatsphäre der Nutzer von Webdiensten und von wissenschaftlichen Arbeiten betrachtet. Neben den beschriebenen Personen-Markierungen wurden vor allem Ortsangaben zu Bildern in der Öffentlichkeit und in der Wissenschaft diskutiert. Wie in Abschnitt 5.1 gezeigt wurde, schützen einige Webdienste diese Informationen gesondert, wenn auch mit deutlichen Makeln. Andere privatsphärerelevante Metadaten, wie zum Beispiel eingebettete Personen-Markierungen, die eindeutige Seriennummer einer Kamera oder andere Nennungen beteiligter Personen, wie der Besitzer einer Kamera, wurden bisher kaum beachtet. Inwieweit zumindest ein Teil dieser Metadaten und ihr Bedrohungspotenzial im Bewusstsein der Nutzer ist, wurde im zweiten Teil der Online-Umfrage betrachtet.

5.3.4.1 Wissen und Nichtwissen der Nutzer

Zu Beginn der Umfrage wurden die Teilnehmer aufgefordert, den Begriff Metadaten zu definieren. Aus gegebenen vier möglichen Definitionen wählten lediglich 61 % der Teilnehmer die korrekte aus. Es kann angenommen werden, dass ebenso wenige oder noch weniger Teilnehmer weitere Details kennen, wie beispielsweise die verschiedenen Möglichkeiten der Speicherung und die jeweiligen Implikationen für die Privatsphäre. Daher wurde für den weiteren Verlauf der Umfrage eine mehr abstrakte Definition des Begriffs verwendet und für die Teilnehmer erläutert: „Metadaten sind Zusatzinformationen zu einem Foto wie Ort, Zeit, Personen, Beschreibung, Titel, Kontext usw. die mit dem Foto gespeichert werden. Die meisten Digitalkameras fügen grundlegende Metadaten wie z. B. Datum, Uhrzeit und Kameramodell schon beim Fotografieren in ein Foto ein.“ Nur ein einzelner Teilnehmer merkte während der Umfrage an, dass kein Unterschied zwischen eingebetteten und anderen Metadaten gemacht worden sei, und dass dies in der Regel einen großen Unterschied mache, wenn es um die Vervielfältigung von Fotos geht.

Um abschätzen zu können, wie die Nutzer mit Metadaten umgehen, wurden die 253 Teilnehmer, die den Begriff Metadaten korrekt definiert hatten, aufgefordert zu verschiedenen Aussagen über ihr Verhalten Stellung zu nehmen. Rund 25 % dieser Teilnehmer gaben an, selbst keine Metadaten zu Fotos hinzuzufügen. Ein gewisser Teil der Teilnehmer wird dies jedoch auch tun, ohne den Begriff der Metadaten zu kennen, wenn sie Fotos in Onlinediensten annotieren. Circa 6 % der 253 Teilnehmer gaben an, alle Metadaten aus Fotos zu löschen, bevor sie die Bilder teilen. Weitere 35 % gaben an, einen Teil der Metadaten vor dem Teilen zu löschen. 2 % von ihnen gaben an, dass ihr Onlinedienste die Metadaten löscht. Die Teilnehmer gaben auch Nichtwissen zu. 58 % von ihnen gaben zu, dass sie nicht wissen, was ihr Fotodienst oder Soziales Onlinenetzwerk mit den Metadaten macht. 29 % gaben zu, nicht zu wissen, was alles in ihren Fotos gespeichert ist, wenn sie diese teilen. Rund 27 % der 253 Teilnehmer gaben an, sich keine Gedanken über Metadaten zu machen, wenn sie Bilder teilen. 9 % der Teilnehmer gaben hingegen an, dass sie Metadaten beim Teilen als eine Bereicherung für alle Betrachter empfinden.

Die Teilnehmer wurden außerdem gefragt, welche Arten von Metadaten sie zu Fotos hinzufügen. Diese Frage wurde dabei nur von den 381 Teilnehmern beantwortet, die zu Beginn der Umfrage angegeben hatten, Fotos per PC oder über mobile Geräte im Web zu teilen. Auf einer 7-Punkte-Skala von *(1) nie* bis *(7) sehr oft* antworteten sie, wie es Abbildung 5.11 zeigt. Die Teilnehmer gaben an, am häufigsten Titel, Beschreibung und Schlagworte zu Bildern hinzuzufügen ($\varnothing = 4{,}3$, $s = 2{,}1$), gefolgt von Namen abgebildeter Personen und groben Ortsangaben (jeweils $\varnothing = 3{,}4$, $s = 1{,}9$). Der Name des Fotografen oder gegebenenfalls der des Kamerabesitzers wird von ihnen selten hinzugefügt ($\varnothing = 1{,}9$, $s = 1{,}4$), jedoch kann dieser innerhalb von

Webdienst oft mit dem hochladenden Nutzer gleichgesetzt werden. Die Teilnehmer gaben an, am seltensten genaue Ortsinformationen zu ihren Bildern hinzuzufügen ($\varnothing = 1{,}8$, $s = 1{,}5$).

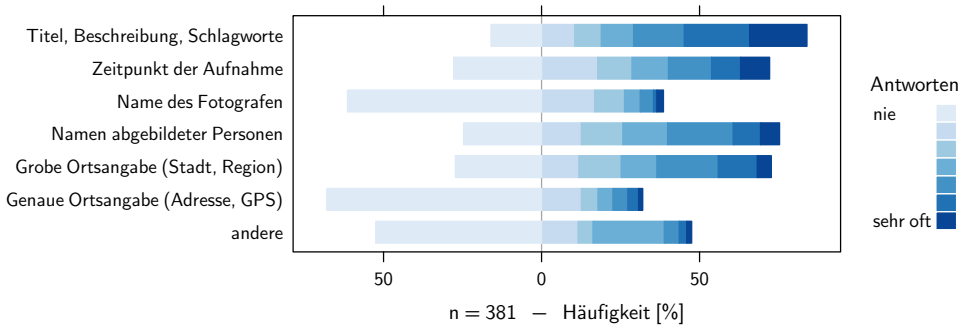


Abbildung 5.11: Häufigkeit mit der die Studienteilnehmer Fotos mit verschiedenen Metadaten annotieren

5.3.4.2 Private Metadaten

Im Rahmen der Umfrage sollte erfasst werden, wie groß die Teilnehmer eine mögliche Verletzung der Privatsphäre durch eine Preisgabe verschiedener Metainformationen einschätzen. Dazu wurden die Teilnehmer aufgefordert zu bewerten, wie groß mögliche Auswirkungen auf die Privatsphäre anderer sein könnten, wenn sie selbst bestimmte Metadaten zu ihren Fotos hinzufügen würden. Außerdem hatten sie die Aufgabe einzuschätzen, wie groß mögliche Auswirkungen auf ihre eigene Privatsphäre sein könnten, wenn andere die entsprechenden Metadaten zu ihren Fotos hinzufügen würden. Bei beiden Fragen bewerteten die Teilnehmer sechs Arten von Metainformationen auf einer 7-Punkte-Skala von *(1) sehr gering* bis *(7) sehr groß*.

Vergleicht man die Antworten der beiden Fragen, stellt man fest, dass die Einschätzungen der Auswirkungen in beiden Fällen nahezu identisch sind. Wie Abbildung 5.12 zeigt, stimmt die Relation zwischen den verschiedenen Metadaten in beiden Fällen überein. Dies zeigt, dass die Teilnehmer ihre eigene und die Privatsphäre Anderer durch dieselben Metadaten ähnlich stark bedroht sehen. Tabelle 5.3 zeigt die durchschnittlichen Einschätzungen für beide Fragen im Detail. Der Rangkorrelationskoeffizient ρ nach Spearman weißt auf eine positive Korrelation der Antworten hin ($0{,}64 < \rho < 0{,}73$, $p < 0{,}001$). Inhaltsbeschreibende Metadaten wie Titel, Beschreibung oder Schlagworte haben laut der Auffassung der Teilnehmer die geringsten Auswirkungen, wie der durchschnittliche Wert von 3 ($s = 1{,}7$) bei beiden Fragen zeigt. Dem Zeitpunkt der Aufnahme ($\varnothing = 3{,}6$, $s = 1{,}7$), dem Namen des Fotografen ($\varnothing = 3{,}4$, $s = 1{,}8$) ebenso wie groben Ortsangaben, wie der Stadt oder der Region in der ein Foto aufgenommen wurde ($\varnothing = 3{,}9$, $s = 1{,}1$), wurden eine leicht geringer als mittlere Bedrohung für die Privatsphäre zugeordnet. Im Vergleich dazu schätzten die Teilnehmer die möglichen Auswirkungen von Namen abgebildeter

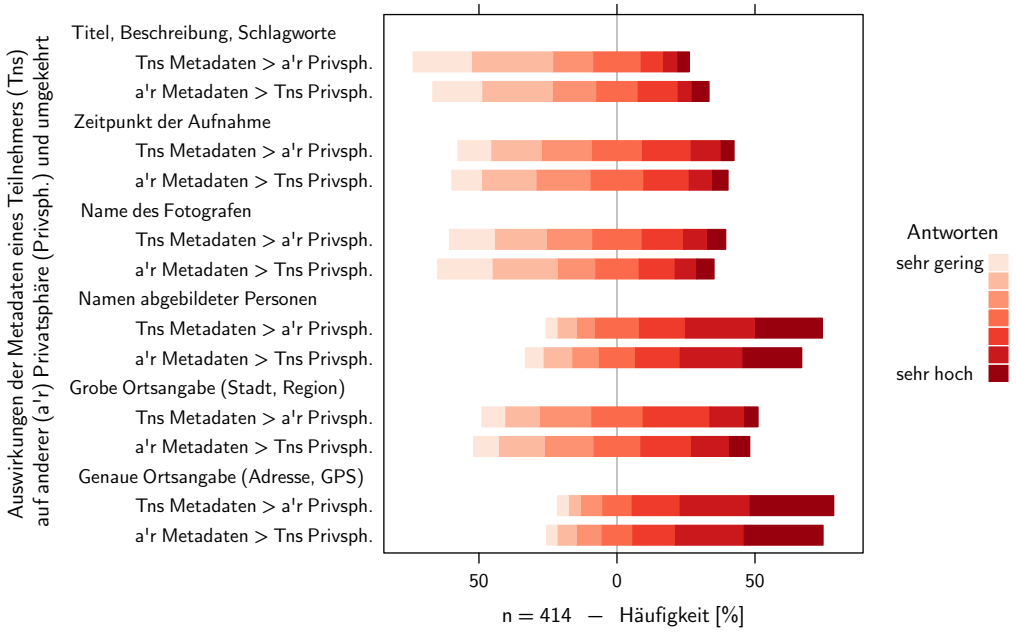


Abbildung 5.12: Mögliche Auswirkungen für die Privatsphäre durch das Hinzufügen verschiedener Foto-Metadaten aus der Sicht des Betroffenen und aus der Sicht des Verursachers

Personen ($\varnothing = 4{,}9$, $s = 1{,}8$) und die genauer Ortsangaben ($\varnothing = 5{,}2$, $s = 1{,}7$), wie einer Postadresse oder von GPS-Koordinaten, höher ein.

Genaue Ortsangaben werden von den Teilnehmern als die Metadaten mit dem größten Bedrohungspotenzial gesehen. Auffällig ist, dass die Teilnehmer einen deutlichen Unterschied zwischen den Namen abgebildeter Personen und dem Namen des Fotografen machen. Beide Informationen geben an, dass die Personen einen Bezug zum Bild haben. Auch die Angabe von Fotografen oder Kamerabesitzern zeigt, dass diese am Ort des Fotos gewesen sind, solange die Kamera nicht verliehen wurde.

Wie Abbildung 5.12 zeigt, gaben die Teilnehmer interessanterweise im Durchschnitt für die meisten Metainformationen an, größere Auswirkungen auf die Privatsphäre anderer durch von ihnen selbst hinzugefügte Metainformationen zu sehen, als es andersherum der Fall war. Für einige, jedoch nicht alle Metainformationen, sind diese Unterschiede statistisch signifikant. Da zudem die Unterschiede der Durchschnittswerte nur gering sind, kann dies lediglich als Indiz gesehen werden, dass die Teilnehmer ihre eigene Privatsphäre eventuell generell weniger gefährdet sehen.

Vergleicht man die Antworten auf die Frage, welche Metainformationen die Teilnehmer zu Fotos hinzufügen mit den Antworten dieser beiden Fragen, lässt sich ein weiterer Trend in den Daten erkennen: Teilnehmer, die angaben Ortsinformationen häufiger zu nutzen, schätzten die möglichen Auswirkungen durch Ortsinformationen als geringer ein (Spearmans $\rho = 0{,}234$, $p < 0{,}001$). Dies kann ein Indiz dafür sein, dass die Verwendung einer Art von Metadaten dazu führt, ihrem Nutzen gegenüber offener zu sein und so weniger Bedenken über mögliche Auswirkungen zu hegen.

Metadaten-Autor Auswirkungen auf	Teilnehmer andere		andere Teilnehmer		*Wilcoxon-Vorzeichen-Rang*		*Spearmans* ρ ($p < 0{,}001$)
	$\varnothing$	s	$\varnothing$	s	z	p	
Titel, Beschreibung, Schlagworte	2,94	1,66	3,23	1,75	−4,739	0,000	0,73
Zeitpunkt der Aufnahme	3,63	1,70	3,59	1,67	−0,478	0,663	0,69
Name des Fotografen	3,49	1,79	3,28	1,83	−3,274	0,001	0,65
Namen abgebildeter Personen	5,08	1,70	4,76	1,87	−4,204	0,000	0,64
grobe Ortsangabe (Stadt, Region)	3,95	1,62	3,90	1,74	−0,902	0,367	0,68
genaue Ortsangabe (Adresse, Koordinaten)	5,31	1,68	5,17	1,75	−2,102	0,036	0,68

Tabelle 5.3: Analyse der Antworten zu möglichen Auswirkungen für die Privatsphäre durch das Hinzufügen verschiedener Foto-Metadaten aus der Sicht des Betroffenen und aus der Sicht des Verursachers

Um die oft diskutierte Preisgabe von Ortsinformationen weiter zu untersuchen, wurde der Einfluss des Publikums in einer weiteren Frage betrachtet. Die Teilnehmer wurden gebeten, ihre persönliche Empfindung zu beschreiben, wenn verschiedene Personen und Webdienste Fotos mit Ortsangaben zu sehen bekämen, auf denen die Teilnehmer abgebildet sind. Zur Beschreibung ihrer Empfindung wurde eine 7-Punkte-Skala von *(1) stört mich gar nicht* über *(4) neutral* bis *(7) stört mich sehr* verwendet. Die Teilnehmer gaben an, mehr oder weniger unbekümmert darüber zu sein, wenn Fotos mit Ortsangaben mit Freunden ($\varnothing = 2{,}24$, $s = 1{,}5$) oder Freunden von Freunden ($\varnothing = 3{,}51$, $s = 1{,}7$) geteilt werden. Bekommen hingegen Fremde diese Bilder zu Gesicht, so stört es die Teilnehmer ($\varnothing = 5{,}16$, $s = 1{,}8$). Ebenso stört es sie, wenn Webdienste – und damit die Dienstanbieter – Zugriff auf Bilder mit Ortsinformationen hätten: Dies gaben die Teilnehmer sowohl für einen Dienst an, der ein geteiltes Bild speichert, um es mit anderen zu teilen ($\varnothing = 5{,}23$, $s = 1{,}9$), sowie für einen Dienst, der ihnen hilft, ihre Privatsphäre zu schützen und dazu aktiv nach Abbildungen ihrer selbst sucht und sie gegebenenfalls informiert ($\varnothing = 5{,}28$, $s = 1{,}9$). Inwieweit dieses starke Unbehagen gegenüber den Diensten mit der Realität übereinstimmt, kann aus der Umfrage nicht abgeleitet werden. Es widerspricht eigentlich sogar der Nutzung von Webdiensten zum Teilen von Bildern. Mit dem Spezialfall eines Privatsphäre-Dienstes befasst sich der dritte Teil der Umfrage genauer.

5.3.4.3 Zusammenfassung

Während Nutzer von Sozialen Onlinenetzwerken wissen, dass sie Kommentare, Ortsinformationen oder Personen-Markierungen zu Bildern im Web hinzufügen können, ist der Begriff der Metadaten nicht allgemein bekannt. Inwieweit dies damit gleichzusetzen ist, dass die Nutzer nicht wissen, dass privatsphärerelevante Informationen

in geteilten Fotos eingebettet sein können, bleibt an dieser Stelle ungeklärt. Die Ergebnisse der Umfrage haben jedoch gezeigt, dass selbst ein nennenswerter Teil derer, die Metadaten kennen, nicht weiß, was in Fotos zum Zeitpunkt des Teilens gespeichert ist oder was Webdienste mit ihren Metadaten tun. Dies unterstreicht die Notwendigkeit, dass Bewusstsein über Foto-Metadaten geschaffen werden muss, um die Privatsphäre der Nutzer durch diese nicht zu gefährden. Während Bedrohungen durch Personen-Markierungen und Ortsangaben vielen bekannt sind, muss den Nutzern deutlich gemacht werden, dass auch andere Informationen Bedrohungen darstellen können, die die Nutzer momentan nur zum Teil sehen. Dies zeigt sowohl die Diskrepanz der Einschätzung von Namen abgebildeter Personen und dem Namen des Fotografen, wie auch die relativ niedrig eingeschätzte Bedrohung durch grobe Ortsangaben. Das Unwissen der Nutzer gibt Anlass zu vermuten, dass durch Aufklärung, die Schaffung von Bewusstsein und von Transparenz der Nutzung, der Speicherung und der Löschung von Metadaten viel zum Schutz der Privatsphäre beigetragen werden kann.

5.3.5 Privatsphäre-Kompromisse

Das traditionelle Verständnis von Privatsphäre im Alltag und in der Forschung hat zum Ziel die Privatsphäre der Nutzer mit allen Mitteln zu schützen und dazu jede persönliche Information, die als privat verstanden werden könnte, vor dem Zugriff durch andere zu bewahren. Das alltäglich beobachtete Verhalten der Nutzer im Web 2.0 und im Social Web, welches vom Mitwirken, dem sich Mitteilen und dem Teilen diverser Inhalte lebt, lässt vermuten, dass dies für viele Nutzer heute nicht mehr in solch einer strengen Form zu gelten scheint. Die Nutzer geben vielerorts bereitwillig persönliche Informationen von sich preis, um Funktionen von Onlinediensten oder mobilen Apps nutzen zu können oder schlichtweg um sich in einem guten Licht darzustellen. Das Verhalten der Nutzer legt den Gedanken nahe, ob die Bereitschaft zur abgewägten Preisgabe nicht ebenso für den Schutz der Privatsphäre verwendet werden kann: Es könnten die einen Informationen preisgegeben werden, um andere Informationen zu schützen.

Foto-Metadaten können eine Vielzahl von Informationen enthalten, die von technischen Daten bis zum Wer, Wann, Was oder Wo eines Bildes reichen. Sie dienen der Erhaltung des nicht sichtbaren Bildkontextes oder der Übersicht großer Bildsammlungen. Sie können Ursache einer Bedrohung sein, jedoch können sie eventuell auch dem Schutz der Privatsphäre dienen. Einen ähnlichen Ansatz verfolgten Klemperer et al. [117]: Sie untersuchten, wie effektiv Schlagworte und Bildtitel als Basis von Zugriffskontrollregeln zum Schutz von Bildern verwendet werden können. In Rahmen dieser Dissertation hingegen sollen Metadaten verwendet werden, um die Privatsphäre der Personen zu schützen, die von einem Bild betroffen sind, indem sie

helfen, die betroffenen Personen zu identifizieren, um sie über die Bilder zu informieren. Die Grundannahme dabei ist, dass der Bildinhalt meist schädlicher für die Privatsphäre ist, als die angefügten Metadaten. Im dritten Teil der durchgeführten Online-Umfrage wurden einige grundlegende Fragen zu diesem Ansatz untersucht.

Sollen persönliche Informationen zum Schutz der Privatsphäre verwendet werden, stellen sich einige fundamentale Fragen zur Privatheit von Informationen, die sich spätestens die Nutzer eines entsprechenden Schutzsystems stellen müssen: Sind Informationen, die von Anderen als privat angesehen werden, ebenso privat für den jeweiligen Nutzer? Insbesondere sind alle Informationen, die vom Nutzer als privat angesehen werden „gleich privat“ in der Hinsicht, dass die Zahl und Auswahl von Personen oder Webdiensten, mit der er diese teilen würde, identisch sind? Ist dem nicht so, welche Informationen würde der Nutzer mit wem teilen und mit wem nicht? Gibt es Unterschiede bezüglich der Privatheit von Informationen, wie es das zuvor beschriebene Verhalten der Nutzer nahe legt, so existieren verschiedene ***Privatheitsstufen***. Jede Stufe enthält Informationen, die ähnlich bedeutsam für die Privatsphäre eines Nutzer sind. Die Einordnung von Informationen ist dabei eine individuelle Entscheidung. Viele nach Westin klassifizierte Privatsphäre-Fundamentalisten und -Unbekümmerte nehmen vermuteterweise nur eine einzige Stufe wahr. Der große Anteil der Privatsphäre-Pragmatisten legt jedoch die Annahme nahe, dass Privatheitsstufen ein sinnvolles Basiskonzept für Schutzmechanismen sein können.

Um diese Idee zu evaluieren, wurden die Teilnehmer der Umfrage gefragt, ob sie alle persönlichen Informationen gleich privat im Sinne von „die gleichen oder gleich viele Personen dürfen etwas erfahren“ einschätzen und folglich der Existenz von Abstufungen zustimmen. Auf der 7-Punkte-Skala von *(1) volle Zustimmung* bis *(7) absolute Ablehnung* mit *(4)* als *neutral* stimmten die Teilnehmer der Existenz mit einem durchschnittlichen Wert von 2,63 ($s = 1{,}7$) zu. 13,5 % der Teilnehmer lehnten ihre Existenz ab; 5,6 % lehnten sie absolut ab. 12,7 % antworteten mit neutral. 74,2 % stimmten der Existenz zu; 33,1 % stimmten voll zu. Ein Zusammenhang zwischen diesen Antworten und der Privacy Segmentation nach Westin konnte nicht festgestellt werden. Die Antworten zeigen, dass die Grundannahme der Existenz von Privatheitsstufen gegeben zu sein scheint. Existieren verschiedene Abstufungen, so können sie zum Schutz der Privatsphäre genutzt werden. Ein Schutzmechanismus kann weniger private Informationen nutzen, um mehr private Informationen zu schützen. Er kann somit von einem ***Privatsphäre-Kompromiss*** profitieren:

> *Existieren verschiedene* Privatheitsstufen *von Informationen in einem System, welches auf der Verwendung von öffentlichen wie auch privaten Informationen basiert, wie es Soziale Onlinenetzwerke und andere Dienste im Social Web tun, können Nutzer für sie weniger private Informationen preisgeben, um auf Basis dieser, andere für sie mehr private Informationen zu schützen.*

In der durchgeführten Umfrage wurden die Teilnehmer gefragt, ob sie solch einer Art von Tausch/Kompromiss zu stimmen würden. Zur Unterstützung der Frage wurde folgendes Beispielszenario gegeben: „Gebe einem Dienst z. B. deinen Aufenthaltsort preis, um Fotos zu erhalten, die dort entstanden sind und dich zeigen könnten." Auf der 7-Punkte-Skala von *(1) volle Zustimmung* mit *(4) neutral* bis *(7) absolute Ablehnung* gaben die Teilnehmer der Umfrage im Durchschnitt ihre Zustimmung zur Nutzung von Privatheitsstufen und dem Eingehen eines Privatsphäre-Kompromisses mit einem Wert von 3,49 ($s = 1{,}7$). 22,7 % der Teilnehmer lehnten einen Kompromiss ab. 24,5 % von ihnen gaben an neutral zu sein und 52,7 % der 414 Teilnehmer stimmten dem Zunutzemachen von Privatheitsstufen zu. Abbildung 5.13 zeigt die Antworten der Teilnehmer zu beiden Fragen zu Abstufungen von Privatheit.

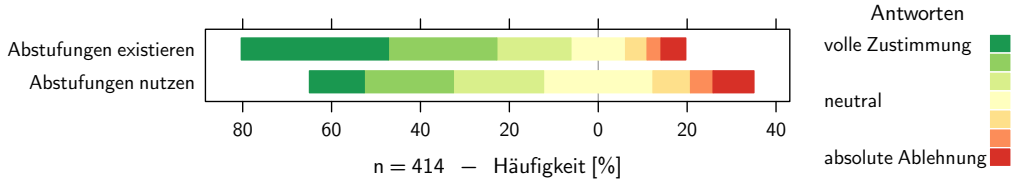


Abbildung 5.13: Wahrnehmung über die Existenz verschiedener Privatheitsabstufungen und Meinung dazu, ob weniger private Informationen zum Schutz mehr privater Informationen genutzt werden dürften

Im Rahmen der Umfrage wurden die Teilnehmer gefragt, welche Informationen sie für Benachrichtigungen über Fotos, auf denen sie zu sehen sein könnten, gegenüber ihren Sozialen Onlinenetzwerk oder einem Fotodienst preisgeben würden. Es wurde die gleiche 7-Punkte-Skala wie zuvor verwendet. Abbildung 5.14 zeigt die Antworten der Teilnehmer. Sie stimmten am stärksten zu, dass ein Dienst ihre sich bereits online befindenden Profilfotos verwenden dürfe ($\varnothing = 2{,}97$, $s = 1{,}8$), um sie über Fotos ihrer selbst zu informieren. Diese könnten beispielsweise verwendet werden, um ein System zur Gesichtserkennung zu trainieren, um es für die Fotosuche zu verwenden. Dienste wie Facebook oder Google+ nutzen diese zum Teil schon, um Personen-Markierungen auf Fotos im Freundeskreis vorzuschlagen. Die Informationen, die die Teilnehmer im Durchschnitt als Zweites für die Fotosuche preisgeben würden, sind durch sie selbst festgelegte Orte auf einer Landkarte, von welchen sie keine Fotos mit sich selbst online haben möchten ($\varnothing = 4{,}0$, $s = 1{,}9$). Diese Orte könnten mit Ortsinformationen in geteilten Fotos abgeglichen werden, um Fotos von Orten wie dem eigenen Zuhause zu vermeiden. Im Durchschnitt waren die Teilnehmer abgeneigt weitere Profilfotos bereitzustellen, die bestimmten Vorgaben entsprechen, wie es beispielsweise Ausweisfotos tun ($\varnothing = 4{,}5$, $s = 1{,}9$). Diese wären eine bessere Basis für das Trainieren von Gesichtserkennungsmethoden. Die Teilnehmer gaben im Durchschnitt an, ebenso leicht abgeneigt zu sein ihre Freundesliste frei zugeben ($\varnothing = 4{,}5$, $s = 1{,}8$), um speziell die Fotos ihrer Freude auf betreffende Fotos hin

zu durchsuchen. Die Teilnehmer der Umfrage waren am stärksten der allgemeinen Vorstellungen gegenüber abgeneigt, ihre aktuelle genaue Position beispielsweise über eine mobile App preiszugeben, wenn sie sich in Situationen beziehungsweise an Orten befinden, von denen sie keine Fotos im Web haben möchten ($\varnothing = 5{,}4$, $s = 1{,}9$). Diese Informationen würden den effektivsten Abgleich mit Ortsinformationen in Fotos ermöglichen, um potenziell bedrohliche Fotos zu finden.

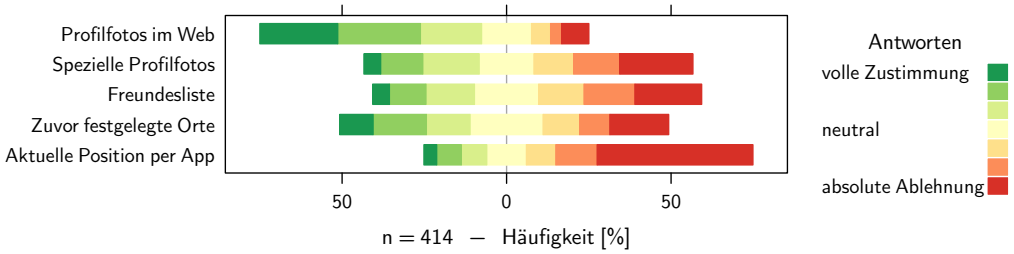


Abbildung 5.14: Welche Informationen die Studienteilnehmer ihrem Sozialen Onlinenetzwerk anvertrauen würden, um Fotos von sich zu finden, die andernfalls verborgen bleiben könnten

Bei einer Betrachtung aller Teilnehmer muss festgestellt werden, dass diese lediglich der Verwendung existierenden Profilbilder zustimmten und sonst im Durchschnitt einen Privatsphäre-Kompromiss ablehnten, wenn es um die Verwendung ihrer eigenen Informationen ging. Betrachtet man jedoch nur die Teilnehmer, die zuvor der Ausnutzung von Privatheitsstufen zustimmten (plus diejenigen, die der Verwendung ihrer Informationen neutral gegenüberstanden), als potenzielle Nutzer eines kompromissbasierten Systems, so stellt sich die Kompromissbereitschaft im Einzelnen wie folgt dar: 67,5 % (82,6 %) würden die Nutzung existierender Profilbilder erlauben und 35 % (51,7 %) würden weitere Profilbilder gemäß bestimmter Vorgaben bereitstellen. 30,9 % (50,5 %) würden die Verwendung ihrer Freundesliste zulassen. 39,6 % (61,8 %) würden auf einer Karte festlegte private Orte für die Suche freigeben und 19,1 % (31,2 %) würden die Nutzung eines standortbezogenen Dienstes in Erwägung ziehen, um ihren aktuellen Ort für die Suche zur Verfügung zustellen.

Um die Wahrnehmung der Teilnehmer bezüglich der Preisgabe ihrer Daten im Rahmen eines Privatsphäre-Kompromisses möglichst gut zu erfassen, wurden diese am Ende der Umfrage um die Bewertung dreier hypothetischer Ausgestaltungen von Kompromissen gebeten. Sie bewerteten die folgenden Aussagen auf einer 7-Punkte-Skala von *(1) volle Zustimmung* mit *(4) neutral* bis *(7) absolute Ablehnung*.

1. „Wenn eine beliebige Person den Ort erfährt, an dem ich gewesen bin, finde ich das nicht so schlimm, als wenn die Person private Fotos von mir zu Gesicht bekommt.“ – Die Teilnehmer stimmten dieser Aussage im Durchschnitt zu ($\varnothing = 3{,}0$, $s = 1{,}6$); 66,2 % von ihnen gaben ihre Zustimmung an und 15,7 % gaben an, dem neutral gegenüberzustehen.

2. „Wenn mein Soziales Onlinenetzwerk den Ort erfährt, an dem ich gewesen bin, empfinde ich das nicht so schlimm, als wenn Freunde und Fremde unerwünschte Fotos zu Gesicht bekommen." – Die Teilnehmer stimmten auch dieser Aussage im Durchschnitt zu ($\varnothing = 3{,}3$, $s = 1{,}8$); 60,4 % von ihnen gaben ihre Zustimmung an und 16,2 % der Teilnehmer gaben die Antwort neutral zu sein.

3. „Wenn es einen Privatsphäre-Dienst gäbe, der mich über Fotos informiert, auf denen ich unerwünschterweise zu sehen bin, indem ich ihm sage, wo ich gewesen bin, so würde ich ihn nutzen. Ich würde ihm sagen, wo ich war, um die Fotos ansehen zu können." – Die Teilnehmer stimmten der Aussage im Durchschnitt zu ($\varnothing = 3{,}7$, $s = 1{,}8$); 53,2 % der Teilnehmer gaben an zuzustimmen und 16,1 % von ihnen standen der Aussage neutral gegenüber.

Abbildung 5.15 visualisiert die Verteilung der Antworten. Die Antworten auf die drei Fragen unterscheiden sich statistisch signifikant (Friedman-Test: $\chi^2_2 = 44{,}46$, $p < 0{,}001$; paarweise Wilcoxon-Tests: $z_{1,2} = -2{,}6$, $p = 0{,}009$; $z_{2,3} = -4{,}3$, $z_{3,1} = -6{,}1$, $p < 0{,}001$). Zwischen den Antworten der ersten beiden Fragen existiert eine leichte Korrelation (Spearmans $\rho_{1,2} = 0{,}596$, $p < 0{,}001$), während die anderen Paare keine erkennbare aufweisen ($\rho_{2,3} = 0{,}24$, $\rho_{3,1} = 0{,}23$, $p < 0{,}001$). Die Teilnehmer stimmten im Allgemeinen den ausformulierten Kompromissen zu. Jedoch waren sie zurückhaltender im Fall der Preisgabe von Informationen an einen Dienst, der sie über potenzielle Fotos von ihnen selbst informiert. Dies kann bedeuten, dass sie Privatsphäre-Kompromisse anerkennen und ihren Nutzen für erstrebenswert halten, sie jedoch nicht allgemein gewillt sind, einem Dienstanbieter zu vertrauen, ihre weniger privaten persönlichen Informationen auch privat zu halten. Dies betont das notwendige Vertrauen, das solch einem Dienst gegenüber geschaffen werden müsste.

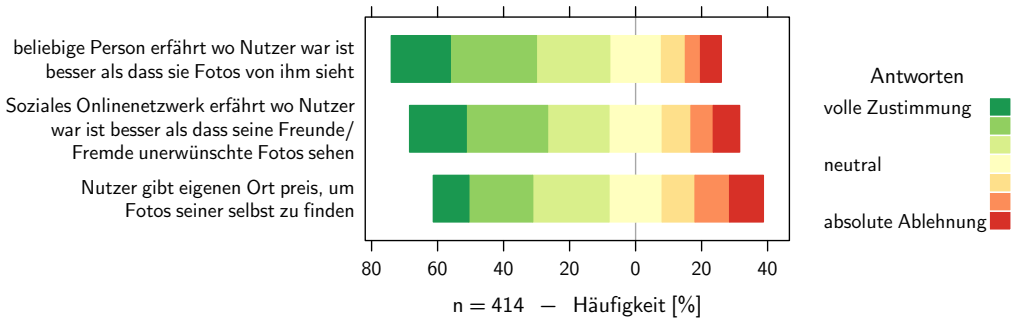


Abbildung 5.15: Wahrnehmung dreier hypothetischer Privatsphäre-Kompromisse

Zusammenfassung

Die Hypothese, dass nicht alle als privat eingestuften Informationen von den Menschen als gleich privat empfunden werden, sondern sich in mehrere Stufen empfundener Privatheit gliedern lassen, wurde durch die Ergebnisse der Umfrage bestätigt. Nur 5,6 % der Teilnehmer lehnten diese Grundannahme absolut ab. Unter der Vor-

aussetzung, dass Privatheitsstufen existieren, können diese zum Schutz der Privatsphäre verwendet werden, indem durch die Preisgabe weniger privat empfundener Informationen andere Informationen, welche als mehr privat eingestuft werden, geschützt werden können. Im Allgemeinen stimmten 77,2 % der Teilnehmer solch einem Privatsphäre-Kompromiss zu oder standen ihm neutral gegenüber. Wurden die Teilnehmer im Folgenden zu möglichen kompromissbasierten Umsetzungen befragt, so war dieser Anteil merklich geringer. Viele Teilnehmer stimmten zu, ihre existierenden Profilbilder gegen die Benachrichtigung über Fotos einzutauschen, jedoch zögerten sie im Durchschnitt bei dem Tausch anderer persönlicher Informationen und dabei besonders im Fall von Ortsinformationen. Ein beachtlicher Anteil der Teilnehmer war jedoch bereit, persönliche Informationen einzutauschen, welche als mögliche Nutzer eines kompromissbasierten Schutzsystems gesehen werden können. Die Ergebnisse zu drei hypothetischen Ausgestaltungen von Kompromissen bestätigten dies: 60,4 % der Teilnehmer gaben an zu bevorzugen, dass ihr Soziales Onlinenetzwerk den Ort erfährt, an dem sie gewesen sind, als wenn Freunde und Fremde unerwünschte Fotos zu Gesicht bekommen. Außerdem gaben 53,2 % der Teilnehmer an einen Dienst nutzen zu wollen, der solch einen kompromissbasierten Schutzmechanismus bietet.

5.3.6 Fazit

Die Ergebnisse der Online-Umfrage geben detaillierte Auskunft über die Wahrnehmung der Nutzer über ihr Bewusstsein über im Web geteilte Fotos. Das erfasste Ausmaß an vorhandenem Bewusstsein sowie die verwendeten Möglichkeiten, sich über Fotos bewusst zu werden zeigen, dass deutlicher Verbesserungsbedarf dafür besteht, Nutzer über geteilte Bilder zu informieren. Es hat sich gezeigt, dass zumindest ein Teil der Nutzer willens ist, zusätzlichen Aufwand in Kauf zu nehmen, um sich über Fotos ihrer selbst bewusst zu werden.

Die Ergebnisse der Umfrage geben Aufschluss über die Wahrnehmung der Privatheit von Metainformationen und der Schwere von Auswirkungen ihrer Preisgabe. Informationen zum Ort eines Fotos und zu betroffenen Personen wurden von den Teilnehmern deutlich als Bedrohung der Privatsphäre angesehen. Andere auch privatsphärerelevante Metadaten hingegen weniger. Auffällig ist, dass die Teilnehmer Namen abgebildeter Personen weitaus bedrohlicher empfanden, als andere Angaben zu potenziell beteiligten Personen, wie der Name des Fotografen. Dies spricht für ein eingeschränktes Verständnis der Informationen und resultierenden Bedrohungen.

Die Teilnehmer stimmten großteils der Annahme zu, dass nicht alle Metainformationen als gleich privat empfunden werden, so dass das vorgestellte Konzept der Privatsphäre-Kompromisse dem Schutz der Privatsphäre dienlich sein könnte. Die Umfrage zeigte, dass ein nennenswerter Anteil der Teilnehmer einen Schutzmechanismus auf Basis eines solchen Kompromisses annehmen könnte. Die Bereitwilligkeit

einen Schutzmechanismus dieser Art zu nutzen hängt dabei vom gebotenen Vorteil ab. Die Teilnehmer schienen interessiert daran, auf Basis eines Privatsphäre-Kompromisses von Fotos ihrer selbst zu erfahren. Sie hatten jedoch auch deutliche Bedenken über die Preisgabe von persönlichen als privat empfundenen Informationen. Das passende Gleichgewicht zwischen Nutzen und Bedenken ist hier sehr wichtig und der entscheidende Faktor für den Erfolg eines Privatsphäre-Dienstes dieser Art.

5.3.7 Exkurs: Faktoren von Privatsphäre-Entscheidungen am Beispiel von Ortsinformationen

Die Teilnehmer der Umfrage machten mit ihren Antworten deutlich, dass in ihren Augen genaue Ortsangaben die größte Bedrohung für die Privatsphäre darstellen. Andere Arbeiten präsentierten hingegen die Grundlage dafür, eventuell Zweifel zu hegen, dass die Preisgabe von Standortinformationen besonders hohe Besorgnis bei den Nutzern hervorruft. Im Kontext von IT-Sicherheit auf mobilen Geräten befand sich die Preisgabe von Ortsinformationen in der unteren Hälfte des „Very-Upset-Rankings“ von 99 Risiken in einer Studie von Porter Felt et al. [130]. Zudem wurde der Aufenthaltsort im Vergleich zu Daten wie dem Adressbuch oder dem Kalender als Information mit dem zweitgeringsten Risiko eingestuft. Ihre Studie beinhaltete außerdem eine Differenzierung des Publikums bei der Risikobewertung: Der dokumentierte Einfluss des Publikums bei der Preisgabe von Ortsinformationen scheint den hier präsentierten Ergebnissen zum Teil ebenfalls zu widersprechen. In einer anderen Publikation fasste Krumm [119] verschiedene Studienergebnisse älterer Publikationen zusammen, deren nahezu einheitliches Ergebnis war, dass sich die Nutzer kaum um die Preisgabe von Ortsinformationen sorgten und dass viele willens waren die kommerzielle Nutzung ihre Daten zu erlauben.

Der auf den ersten Blick erscheinende Widerspruch der Aussagen über die empfundene Privatheit von Ortsinformationen in den verschiedenen Studien verlangt nach einer Erklärung und damit nach einer genaueren Betrachtung. Ein kritischer Vergleich der Arbeiten zeigt, dass die empfundene Privatheit persönlicher Informationen nicht uneingeschränkt verglichen werden darf, da Unterschiede zwischen den Teilnehmern und Unterschiede im Studiendesign auch zu deutlich unterschiedlichen Ergebnissen führen können, wie sich hier im Fall der Preisgabe von Ortsinformationen darstellt. Im betrachteten konkreten Fall mögen sich zuallererst die (deutschen) Teilnehmer und ihre Wahrnehmung von Privatsphäre zu denen der anderen Studien unterscheiden. Des Weiteren behandeln die Arbeiten die Privatheit von Ortsinformationen in verschiedenen Kontexten. Die Arbeiten, die Krumm anführt, fokussierten sich beispielsweise auf den Bereich der Verkehrsüberwachung, auf teils theoretische, frühe standortbezogene Dienste oder auf die Aufzeichnung von Bewegungsprofilen mittels GPS-Trackern zu Forschungszwecken. Porter Felt et al. untersuchten hin-

gegen Risiken des Missbrauchs persönlicher Informationen durch Apps auf mobilen Geräten. Sie vergleichen in ihrer Arbeit die Preisgabe von Ortsinformationen mit anderen Risiken, wie der Preisgabe des eigenen Adressbuchs oder der auf einem Gerät gespeicherten Fotos. Die hier präsentierte Umfrage beschäftigt sich dagegen mit Ortsinformationen zu Fotos, die im Web geteilt werden. In diesem Fall stehen Ortsinformationen nicht für sich alleine, sondern sind an ein Bild und eventuell an weitere Metadaten geknüpft. Fotos sind visuell und für den Nutzer – vielleicht durch die traditionelle Ausbelichtung auf Papier – greifbarer, wenn man es mit anderen Anwendungen wie etwa der Abfrage des Wetters am aktuellen Aufenthaltsort vergleicht. Auch die alltägliche Vertrautheit mit Fotos mag die Wahrnehmung und Privatsphäre-Einordnung der Nutzer beeinflussen.

Die Unterschiede der Teilnehmer und die der Kontexte können neben dem Studiendesign einen bedeutenden Einfluss auf die Wahrnehmung der Privatheit einer persönlichen Information haben und damit einen Einfluss auf Privatsphäre-Entscheidungen ausüben. Diese wurden bisher in der Forschung nicht genauer betrachtet. Als Basis einer grundlegenden Betrachtung werden im Folgenden sieben potenzielle Faktoren vorgestellt, die Einfluss auf die Wahrnehmung der Privatheit ein und derselben persönlichen Informationen in verschiedenen Szenarien/Studien nehmen können und damit eine mögliche Erklärung für die Diskrepanz der genannten Ergebnisse bieten. Die weitere Untersuchung der vorgestellten Faktoren [100] obliegt weiterer Forschung im Bereich der Mensch-Maschine-Interaktion.

Lebensdauer der Informationen / des Transportmediums Ein deutlicher Unterschied zwischen den Studien ist das Medium, über das die Ortsinformationen transportiert werden. Werden beispielsweise Ortsinformationen mit einem standortbezogenen Dienst geteilt, um ein Café in der Nähe zu finden oder den eigenen Standort mit anderen zu teilen, so löst dies keine großen Bedenken bei den Nutzern aus, während im Web geteilte Fotos mit Ortsbezug dies tun. Eine mögliche Erklärung für diesen Unterschied ist die von den Nutzern wahrgenommene Lebensdauer der preisgegebenen Informationen, die mit dem verwendeten Medium zusammenhängt. Es ist anzunehmen, dass es aus der Sicht der Nutzer einen deutlichen Unterschied dazwischen gibt, ob Informationen nur im Rahmen eines Dienstes verfügbar sind, und ob eine Ortsangabe mit einem anderen Datum, wie einem Foto, geteilt, gespeichert und vervielfältigt wird. Während in beiden Fällen die Informationen beschränkt oder sogar weltöffentlich sein können, können die Nutzer der Meinung sein, dass Fotos langlebiger sind und somit eine wahrscheinlichere Bedrohung darstellen.

Publikum Andere Arbeiten haben gezeigt, dass die Menschen Bedrohungen durch Fotos durch quasi jede andere Person wahrnehmen, weder beschränkt auf enge Freunde noch auf fremde Personen. Bekannte Dienstanbieter wie Facebook, jedoch auch

eher unbekannte Anbieter, wie der Wetterdienst hinter einer Wettervorhersage-App, sind auch Teil des Publikums, das über diverse Kanäle Standortinformationen von Nutzern erhält. Das jeweilige Publikum und dessen implizierte Vertrauenswürdigkeit beeinflussen die Bedenken der Nutzer in Bezug auf die Wahrung ihrer Privatsphäre und damit die Entscheidung, ob Ortsinformationen preisgegeben werden oder nicht. Das Very-Upset-Ranking von Porter Felt et al. in [130] zeigte eine eindeutige Abhängigkeit der Wahrnehmung der Privatheit von Ortsinformationen vom Publikum: Während 72 % der Studienteilnehmer angaben sehr verärgert zu sein, wenn Ortsinformationen öffentlich geteilt werden, waren nur rund 60 % über Preisgaben an Freunde und Werbeanbieter sehr verärgert. Und nur 30 % gaben an sehr verärgert zu sein, wenn diese Informationen mit dem Anbieter eines Dienstes geteilt werden. Die Teilnehmer der zuvor präsentieren Online-Umfrage bekundeten wenig Besorgnis darüber, dass Fotos mit Ortsangaben mit Freunden geteilt werden, jedoch zeigten sie deutliches Missempfinden darüber, dass Fremde oder auch Webdienste Zugang zu solchen Fotos bekommen. Diese beiden Beispiele zeigen den Einfluss des Publikums. Sie unterscheiden sich jedoch deutlich: Während die Teilnehmer der Online-Umfrage die stärksten Bedenken im Fall von Dienstanbietern hatten, verursachten genau diese die geringsten Bedenken in der Studie von Porter Felt et al. Dies mag auf die anderen Faktoren zurückzuführen sein.

Persönlicher Nutzen Der persönliche Nutzen oder Gewinn kann ebenfalls ein beeinflussender Faktor sein. Die Nutzer wägen ihren durch die Preisgabe entstehenden persönlichen Nutzen gegen mögliche Bedrohungen ihrer Privatsphäre ab, wenn sie sich für oder gegen eine Preisgabe ihres Standortes entscheiden. Fisher et al. [95] haben gezeigt, dass iOS-Nutzer abhängig vom Zweck einer App entschieden, welcher App sie erlauben, ihren aktuellen Aufenthaltsort zu verwenden. Ihre Teilnehmer erlaubten Apps wie *Maps* oder *Foursquare* häufiger den Zugriff auf Ortsinformationen, während sie haderten, Apps wie dem Musik-Identifikationsdienst *Shazam* diese Informationen zur Verfügung zu stellen. Der wahrgenommene persönliche Nutzen hat keinen direkten Einfluss auf die Wahrnehmung der Privatheit, jedoch kann er einen Einfluss auf die letztendliche Entscheidung über eine Preisgabe haben.

Beziehung zwischen Sender und Information Die Beziehung zwischen demjenigen, der eine Information teilt, und demjenigen, über den die Information geteilt wird, hat vermuteterweise einen Einfluss auf die Wahrnehmung der Privatheit der geteilten Information. Ist jemand fähig Ortsinformationen über jemand anderen zu veröffentlichen, ohne eine Einwilligung dieser Person zu haben, könnte dies zu größerem Schaden führen, als wenn die Person selbst die Information wissentlich preisgibt. So kann jemand ein Foto mit Ortsbezug veröffentlichen, auf dem eine andere Person abgebildet ist, die jedoch keinen Einfluss auf das Teilen hat. Dies mag für die Per-

son bedrohlicher wirken, als wenn sie das Bild selbst teilen würde. Einen ähnlichen Sachverhalt betrachtete die zuvor präsentierte Studie: Sie verglich die Fälle, dass andere Informationen über einen Nutzer teilen damit, dass der Nutzer Informationen über andere teilt. Dabei zeigte sich der Trend, dass die Teilnehmer eine größere Bedrohung für andere durch sich sahen als andersherum. Ahern et al. [71] berichteten Ähnliches von ihrer Studie: Ihre Interviewteilnehmer nannten bei der Abwägung, ob ein Foto öffentlich oder eingeschränkt sichtbar sein sollte, häufiger Auswirkungen für andere Betroffene als für sich selbst.

Kultur und Gesellschaft Ein weiterer potenzieller Faktor der Wahrnehmung der Privatheit von Informationen ist die verschieden ausgeprägte Wahrnehmung von Privatsphäre im Allgemeinen, die durch kulturelle und gesellschaftliche Unterschiede begründet ist. Ein Beispiel, welches diese These unterstützt, bieten Wang et al. [146], die im Rahmen einer Studie Unterschiede in der wahrgenommenen Privatheit von Ortsangaben vom Detailgrad Stadt oder Straße zwischen amerikanischen, chinesischen und indischen Teilnehmern gezeigt haben. Während bis dato die Teilnehmer sehr vieler Privatsphäre-Studien innerhalb der USA rekrutiert wurden, kamen die Teilnehmer der hier präsentierten Studie aus Deutschland. In vielerlei Hinsicht mag sich die Kultur von Amerika und Deutschland nicht so stark unterscheiden, als wenn man westliche und asiatische Kulturen vergleicht, jedoch ist allgemein bekannt, dass die Deutschen ein stark ausgeprägtes Bedürfnis nach Privatsphäre haben.

Persönlicher Kontext Das Wissen eines Nutzers und seine Erfahrungen mit einer Art persönlicher Informationen mag ebenfalls ihre wahrgenommene Privatheit beeinflussen. So ist zu vermuten, dass Personen, die Ortsangaben hin und wieder aktiv nutzen, weniger Bedenken über mögliche Bedrohungen ihrer Privatsphäre durch Ortsinformationen haben. Ein solcher Zusammenhang kann auf Aufgeklärtheit oder auch auf Fehlwissen basieren. Die präsentierten Ergebnisse der Online-Umfrage deuten vage auf einen entsprechenden Zusammenhang hin: Teilnehmer, die angaben Ortsinformationen häufiger zu nutzen, schätzten mögliche Auswirkungen durch solche als geringer ein.

Das Allgemeinwissen der Nutzer über preisgegebene Informationen beeinflusst ebenfalls die Entscheidungsfindung. In der Online-Umfrage gaben 29 % der Teilnehmer, denen das Konzept von Metadaten bekannt war, an, nicht zu wissen, was alles in ihren Bildern gespeichert ist. Ohne dies zu wissen, können sie entsprechend keine informierte Entscheidung fällen. Ein Realbeispiel dafür zeigte der Fall von John McAfee [20], in dem ein veröffentlichtes Foto verriet, wo sich dieser während seiner Flucht aufgehalten hatte, weil ein Journalist nicht wusste oder bedachte, dass sein Smartphone den Ort der Aufnahme im Bild speichert und er dies mit dem Bild zusammen veröffentlichte.

Wird eine Ortsinformation im Kontext anderer Informationen verwendet, beispielsweise in ein Bild eingebettet oder als Annotation eines Mikroblog-Beitrags, so beeinflusst auch der Inhalt dieses Kontextes die empfundene Privatheit der Ortsinformation. Ahern et al. [71] berichteten, dass sich Eltern im Rahmen ihrer Studie als besonders besorgt darstellten, wenn Ortsinformationen zu Bildern von Kindern veröffentlicht wurden.

Greifbarkeit Der Vergleich der Studien legt nahe, dass auch die Greifbarkeit des Mediums, durch welches eine Ortsinformation geteilt wird, einen Einfluss auf die empfundene Privatheit ausübt. Die präsentierte Online-Umfrage befasste sich mit dem Szenario des Teilens von Fotos im Web. In diesem Fall sind Ortsinformationen an den visuellen Inhalt des Bildes gebunden. Digitale Bilder können nicht direkt in die Hand genommen werden, jedoch sind sie viel konkreter und somit für die Nutzer greifbarer als ein Paar von GPS-Koordinaten, das an einen Webdienst gesendet und dort aufgezeichnet wird, wie es in den Szenarien der anderen genannten Studien der Fall war. Im Fall von standortbezogenen Diensten, wie auch im Fall des Missbrauchs von Zugriffsrechten für Ortsinformationen durch mobile Apps, ist die Verwendung einer Ortsinformation im Gesamtszenario sowie das Wie und Wo ihrer Speicherung für den Nutzer weitaus weniger verständlich, geschweige denn nachvollziehbar.

Fazit

Auch wenn die Untersuchung der Privatheit persönlicher Informationen und ihre Stellung im Kontext des Privatsphäreschutzes schon in einer Vielzahl von Arbeiten untersucht wurden, gibt es insbesondere menschliche Faktoren, die bisher nur wenig betrachtet wurden. Für ein voll umfassendes Verständnis müssen auch diese weiter untersucht werden, wie dieser Exkurs verdeutlicht.

5.4 Studie zum Bewusstsein über geteilte Fotos am Beispiel von Facebook

Die Online-Umfrage in Abschnitt 5.3 hat gezeigt, dass sich die Menschen nicht ausreichend über Fotos Anderer informiert fühlen, die ihre Privatsphäre beeinflussen könnten. Sie wünschen sich weitere Unterstützung dabei, möglichen Bedrohungen verursacht durch Bilder anderer Nutzer zu begegnen. Neben technischen Lösungen zur Einflussnahme auf die Bilder von Anderen [78, 136] werden Maßnahmen zur Schaffung von Bewusstsein über potenziell bedrohliche Bilder benötigt. Zuallererst muss jedoch dafür gesorgt werden, dass sich die Nutzer überhaupt bewusst sind, dass mögliche Bedrohungen ihrer Privatsphäre durch Bilder Anderer existieren, da sie sonst keinen Anlass sehen zu handeln. Bedrohungen dieser Art sind zwar allge-

mein bekannt, jedoch scheinen sich viele Nutzer nicht persönlich betroffen zu fühlen. Den Nutzern muss bewusst gemacht werden, welches Ausmaß die bedrohlichen Inhalte haben können, dass ihre Privatsphäre eventuell stärker als angenommen bedroht ist, und dass sie den Bedrohungen womöglich oft nicht allein durch ein wenig Aufmerksamkeit begegnen können. Eine Erfassung des Ausmaßes ist außerdem für die Forschung von hohem Interesse, damit die Motivation weiterer Arbeiten nicht allein auf Vermutungen oder auf Selbstauskünfte der Nutzer gestützt werden muss.

Um diese Aspekte zu adressieren, wurde die Facebook-App *Foto-Privatsphäre-Statistik* erstellt. Die App ermöglicht Facebook-Nutzern zu erfahren, wie groß das Ausmaß potenziell bedrohlicher Fotos und assoziierter Metadaten ist. Sie beschränkt sich dabei für eine erste Näherung auf die Fotos direkter Freunde. Auf Basis der App wurde eine Studie [104] durchgeführt, die zusammen mit den Ergebnissen in diesem Abschnitt vorgestellt wird. Während vorherige Arbeiten das Bewusstsein der Menschen häufig auf Basis von Selbstauskünften untersuchten, wurde im Rahmen der Studie das Ausmaß der möglichen Bedrohung durch Fotos Anderer in Form realer Zahlen erfasst und das Bewusstsein der Nutzer – ihr Wissen über das Ausmaß – gemessen. Hierzu wurden die realen Werte für jeden Nutzer durch die App bestimmt und die Nutzer um Schätzungen einiger Werte gebeten, so dass über die Diskrepanz zwischen Realwerten und Schätzwerten Schlüsse über das vorhandene Bewusstsein über das Ausmaß der Quelle möglicher Bedrohungen gezogen werden konnten.

Diskussion empirischer Daten Sowohl für die Antworten der Teilnehmer als auch für die gesammelten Facebook-Daten zeigten Normalitätstests (Shapiro-Wilk, D'Agostino), Histogramme und Quantile eine statistisch signifikante Abweichung der Daten von der Normalverteilung. Folglich werden nicht-parametrische Tests für die Analyse der Ergebnisse verwendet. Im Folgenden werden vor allem Quantile und die mittlere absolute Abweichung vom Median (kurz: MAD) verwendet, um die Verteilung der Daten und Antworten zu beschreiben. Der Durchschnitt $\varnothing$ und die Standardabweichung s werden ebenfalls verwendet, wenn Ergebnisse mit vorherigen Ergebnissen verglichen werden, die ebenfalls diese Maße verwendete haben. Alle erfassten p-Werte sind so gering, dass die als statistisch signifikant beschriebenen Ergebnisse auch unter Einbeziehung der Bonferroni-Korrektur eine statistische Signifikanz aufweisen.

5.4.1 Studiendesign

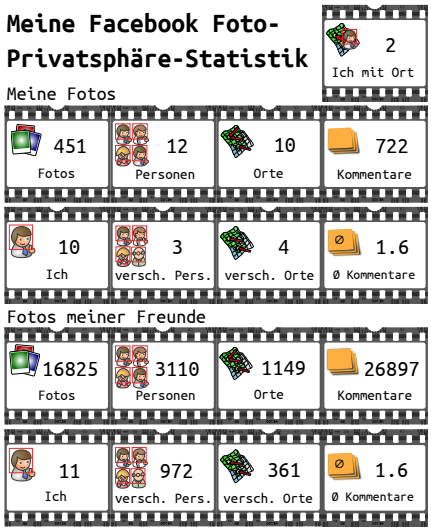
Die Studie bestand aus der Ausführung der Facebook-App und der Beantwortung zweier optionaler Fragebögen. Sowohl die App als auch die Fragebögen waren auf Deutsch und Englisch verfügbar, um ein größeres Publikum ansprechen zu können. Die Teilnahme an der Studie war freiwillig und ohne weitere Gegenleistung. Die

Motivation zur Teilnahme war somit nur das Bekommen der eigenen Foto-Statistik. Aus Sicht der Nutzer und in der Bewerbung der App stand die App selbst im Vordergrund. Die Studie wurde als Nebenprodukt für die Forschung jedoch deutlich beschrieben und die Nutzer wurden über den korrekten Umgang mit ihren Daten aufgeklärt. Ergänzende Informationen zur Funktion der App und die Fragebögen sind in Anhang C.2 zu finden.

Zu Beginn der Ausführung der Facebook-App *Foto-Privatsphäre-Statistik* wurden die App-Nutzer gebeten, den ersten Fragebogen auszufüllen. Dieser *Pre*-Fragebogen erfragte Schätzungen der Nutzer über die Zahl der Fotos, die ihre Freunde teilen, sowie die Menge von Personen-Markierungen und Ortsangaben dieser Bilder. Nach dem Ausfüllen oder Überspringen des Fragebogens startete die App die Berechnung der Statistik für den ausführenden Nutzer. Da die Facebook-API einige notwendige Funktionen nicht implementierte beziehungsweise einige Auswertungen sehr aufwändig waren, wurden die notwendigen Informationen über die API bezogen, anonymisiert gespeichert und auf dem System der App ausgewertet. Angaben zu den Fotos des Nutzers wurden zuerst ermittelt und auf Basis von AJAX direkt im Webbrowser angezeigt. Da die Auswertung der Fotos der Freunde eines Nutzers einen deutlich größeren Zeitraum in Anspruch nahm, wurde die Berechnung im Hintergrund ausgeführt. Nach der Fertigstellung der Statistik des Nutzers wurde der Nutzer über eine hinterlassene E-Mail-Adresse oder durch eine Facebook-Benachrichtigung darüber informiert. Über einen Weblink konnte er seine persönliche Statistik daraufhin betrachten. Abbildung 5.16 zeigt ein reales Ergebnis eines Nutzer mit einer innerhalb des gewonnenen Datensatzes durchschnittlichen Anzahl von Freunden, so wie es dem Nutzer angezeigt wurde. Die Seite zur Visualisierung des persönlichen Ergebnisses bot außerdem die Möglichkeit, Bild und Text, wie sie die Abbildung zeigt, zusammen mit einem persönlichen Kommentar in der Chronik des Nutzers zu veröffentlichen, um unter seinen Freunden Bewusstsein über mögliche Probleme zu schaffen und um die App selbst zu verbreiten. Die Ergebnisbenachrichtigung enthielt außerdem eine Einladung zum zweiten Fragebogen. Dieser *Post*-Fragebogen erfasste die Empfindungen der Nutzer über die realen Ergebnisse. Zudem wiederholte er einzelne generelle Fragen zum Bewusstsein über Fotos im Web aus der Online-Umfrage in Abschnitt 5.3, um deren Ergebnisse in einem anderen Nutzerkreis zu überprüfen.

5.4.2 Teilnehmer-Rekrutierung

Um eine möglichst breite Streuung der App und der Studienteilnehmer zu erlangen, wurden die Teilnehmer über verschiedene Wege rekrutiert. Zu Beginn der Studie wurden Teilnehmer vorwiegend aus den Freundeskreisen und Facebook-Freunden der Mitglieder der Arbeitsgruppe Distributed Computing & Security über Gespräche, E-Mails und die Veröffentlichung persönlicher Ergebnisse in Facebook-Chroniken ak-



„Meine Freunde teilen mindestens 16.825 Fotos, auf denen 3.110 Personen- und 1.149 Ortsmarkierungen sind. 26.897 Kommentare wurden gemacht.

Ich wurde 10-mal markiert sowie 972 andere Personen. 361 verschiedene Orte wurden markiert. Ich wurde 2-mal auf Fotos mit Ortsangabe markiert.

Und du? Nutze die Foto-Privatsphäre-Statistik-App und finde es heraus.

18,2 % meiner Freunde teilen keine Fotos oder haben den Zugriff für Apps gesperrt.“

Abbildung 5.16: Facebook-App Foto-Privatsphäre-Statistik: Übersichtsbild und generierter Text der *Poste-in-Chronik*-Funktion eines Nutzers mit durchschnittlicher Freundesanzahl

quiriert. Hierdurch wurden Ergebnisse für 113 Personen gewonnen, die vorwiegend Mitarbeiter und Studierende der Universität waren. Diese werden im Weiteren als *initiale Nutzer* referenziert. Im Folgenden gab die Leibniz Universität Hannover eine Pressemeldung über die App heraus [27]. Aus dieser entstand ein Radiointerview über die App, welches vom öffentlich-rechtlichen Sender Deutschlandradio im Hörfunkprogramm *DRadio Wissen* am Thementag *Privatsache* gesendet und online zur Verfügung gestellt wurde [10]. Durch die Sendung wurden weitere 79 Nutzer gewonnen, die die zweite Teilnehmergruppe *DRadiohörer* bilden. In Folge der Radiosendung entstand ein Online-Artikel über die App im Resort Internet von Bild Online [2], der Nachrichten-Webseite der größten deutschen Regenbogenpresse-Zeitung. Dieser Artikel generierte einen großen Teil der folgenden 2.561 App-Nutzer, von denen mindestens 1.698 Personen laut Facebook-Profilangaben aus Deutschland kamen. In dieser letzten Phase wurden zudem vermehrt internationale Nutzer gewonnen. Dies ist neben weiteren kleinen Web-Artikeln zur App vermutlich darauf zurückzuführen, dass die gestiegene Nutzerzahl dafür sorgte, dass die App in Facebooks *App-Zentrum* gelistet wurde und auch über die Facebook-Suche zu finden war. Da ein Großteil der Nutzer jedoch aus dem Beitrag auf Bild Online resultierte, wird diese Nutzergruppe im Weiteren als *Bildleser* referenziert.

Insgesamt nutzten bis zum Zeitpunkt der Datenanalyse 2.753 Personen die App. 2.275 von ihnen beantworteten mindestens eine Teilfrage des Pre-Fragebogens. 2.245 Personen schätzten die Menge der geteilten Fotos, die Menge der assoziierten Ortsangaben oder Personen-Markierungen. Der Post-Fragebogen wurde von 269 Personen beantwortet.

5.4.3 Demographie

Von den 2.753 App-Nutzern gaben 84,5 % an männlich zu sein, 15,1 % weiblich und 0,4 % von ihnen hatten ihr Geschlecht nicht in ihrem Facebook-Profil angegeben. Im Pre-Fragebogen gaben 2.139 Personen ihr Alter an. Ihr Alter reichte von 13 Jahren bis hin zu 77 Jahren (Modus = 26, Median = 30, MAD = 10,4). Die Korrektheit der sehr niedrigen und hohen Angaben wurde durch manuelle Prüfung öffentlicher Profilbildern verifiziert, um absichtliche Falschangaben weitestgehend auszuschließen. Das Alter der Nutzer wurde nicht von Facebook bezogen, da dies die Berechtigung für persönliche Detailinformationen notwendig gemacht hätte. Da die meisten Teilnehmer über deutsche Online-Nachrichten rekrutiert wurden, kam ein Großteil der Nutzer aus deutschsprachigen Ländern. Mindestens 64,4 % der Nutzer kamen aus Deutschland (27 % laut Facebook-Profilangaben, 37,4 % gemäß der Geokodierung ihrer Client-IP-Adresse). Weitere 1,2 % waren aus Österreich, 1 % aus der Schweiz und 0,4 % aus den Niederlanden. Das häufigste nicht deutschsprachige Land waren die USA, aus denen 0,6 % der Nutzer stammten. Für 28,6 % der Nutzer konnte das Wohn- oder Ursprungsland nicht festgestellt werden. Die übrigen 3,8 % kamen aus 40 weiteren Ländern aller Kontinente.

Da einige Fragen des Post-Fragebogens mit der vorherigen Online-Umfrage aus Abschnitt 5.3 verglichen werden, wurde die Teilnehmerzusammensetzung dieser 269 Personen nochmals separat analysiert: 78,8 % der Post-Fragebogen-Teilnehmer gaben an männlich zu sein, 20,8 % weiblich und 0,4 % von ihnen machten keine Angabe. Ihr Alter reichte von 13 bis 76 Jahre (Modus = 26, Median = 31). Mindestens 67,3 % von diesen kamen aus Deutschland, 6,3 % aus anderen Ländern und die übrigen ließen keine Rückschlüsse auf ihre Herkunft zu.

5.4.4 Fotos der App-Nutzer und ihrer Freunde

Durch die Erhebung der Foto-Privatsphäre-Statistiken der 2.753 App-Nutzer hatte die Facebook-App Zugriff auf rund 75,7 Millionen Fotos. Entsprechend der Datenschutzerklärung wurde auf die Bilder selbst nie zugegriffen, sondern es wurden nur die zu ihnen gespeicherten Informationen verarbeitet. Die 75,7 Millionen erfassten Fotos stammten von den 2.753 App-Nutzern selbst sowie von 572 Tausend ihrer 817 Tausend Freunde. Ungefähr 30 % der Freunde teilten keine Fotos oder hatten den Zugriff für Apps, welche ihre Freunde nutzen, deaktiviert. 99,2 % der erfassten Bilder stammten von Freunden der Nutzer. Im Durchschnitt hatten die Nutzer 296 Freunde. Die Verteilung der Zahl der Freunde wird durch folgende Quantile beschrieben: $Q_{0,25} = 116$, $Q_{0,5} = 221$, $Q_{0,75} = 383$, und $Q_{0,95} = 738$. Der Nutzer mit den meisten Freunden hatte 5.405 Freunde.

11,3 % (8,5 Millionen) aller Fotos waren mit Ortsangaben versehen. 610 Tausend verschiedene Orte wurden durchschnittlich 14-mal als Ortsangabe von Bildern ver-

wendet. 55,7 % dieser Orte wurden lediglich einmal verwendet, 13 % zweimal und 11,4 % der Orte traten jeweils drei- bis fünfmal auf. Die Häufigkeitsverteilung der Orte hat einen langen Rattenschwanz ($Q_{0,9} = 19$, $Q_{0,95} = 48$, $Q_{0,99} = 170$). Der am häufigsten verwendete Ort „Berlin“ trat 90.837-mal auf.

In 22,4 % (17 Millionen) aller Fotos war mindestens eine Person markiert und die Markierung mit ihrem Facebook-Profil verknüpft. Diese Markierungen beinhalten Bilder, auf denen eine Person markiert worden ist und ebenso Erwähnungen wie eine Profilverknüpfung in einer Bildbeschreibung. Zusätzliche 0,5 % aller Fotos enthielten mindestens eine nicht verknüpfte textuelle Markierung. 0,8 % aller Fotos enthielten sowohl nicht verknüpfte als auch profilverknüpfte Markierungen. In Summe enthielten die Fotos mit Personen-Markierungen 35 Millionen Markierungen (davon 34 Millionen mit Profilverknüpfungen). Jedes Bild hatte durchschnittlich zwei Markierungen. Das Foto mit den meisten Markierungen enthielt 205 Stück. Die Anzahl der Markierungen pro Bild war wie folgt verteilt: 56,2 % der Fotos enthielten eine Markierung; 25,2 % hatten zwei Markierungen, 8,7 % hatten drei, 4 % hatten vier Markierungen, 1,9 % hatten fünf, 2,7 % von ihnen hatten sechs bis zehn Markierungen und 1,3 % enthielten mehr als zehn Markierungen.

6,3 Millionen verschiedene Personen waren insgesamt auf den Bildern markiert. Wie häufig jede Person markiert war, beschreiben die folgenden Quantile: $Q_{0,25} = 1$, $Q_{0,5} = 2$, $Q_{0,75} = 4$, $Q_{0,95} = 199$. Die Person, die am häufigsten markiert wurde, wurde 6.229-mal markiert. Es darf jedoch nicht vergessen werden, dass diese Zahlen nur untere Schranken darstellen, da Fotos von Freunden auch Markierungen von Freunden von Freunden enthalten, die sehr wahrscheinlich auch auf weiteren Fotos markiert waren, die außerhalb des Zugriffs der App lagen. Beschränkt man die Analyse der Daten auf die App-Nutzer, so waren 2.421 von ihnen (87,9 %) mit folgenden Häufigkeiten auf ihren Fotos und den Fotos ihrer Freunde markiert: 18,3 % bis zu dreimal, 21,4 % vier- bis zehnmal und 60,3 % von ihnen waren mehr als zehnmal markiert. Die Verteilung hat abermals einen Rattenschwanz wie die Quantile zeigen: $Q_{0,5} = 16$, $Q_{0,75} = 38$, $Q_{0,9} = 88$, $Q_{0,95} = 136$. Beschränkt man die Auswahl auf Fotos mit Personen-Markierungen der App-Nutzer, welche jeweils auch eine Ortsangabe hatten, so waren 1.758 Nutzer (63,9 %) auf mindestens einem solchen Foto markiert. 22,5 % der Nutzer waren auf genau einem solchen Foto markiert. 14,3 % von ihnen auf zwei Fotos und 10,2 % von ihnen waren auf drei Fotos mit Ortsangaben markiert. Insgesamt waren 74,6 % der markierten App-Nutzer auf bis zu zehn solcher Fotos markiert, während die übrigen 25,4 % in Form eines langen Rattenschwanzes verteilt waren: $Q_{0,9} = 23$, $Q_{0,95} = 42$. Auf 573 Fotos mit Ortsmarkierungen war die Person mit den meisten kombinierten Orts- und Personenmetadaten markiert.

Kommentare und Bildtitel können Informationen enthalten, die ebenfalls die Privatsphäre eines Nutzers beeinträchtigen können. 28,3 % aller Fotos hatten mindes-

tens einen Kommentar. Die durchschnittliche Anzahl an Kommentaren dieser Fotos war 4,5 und das Maximum an Kommentaren zu einem Bild war 20.244. Die Verteilung der Kommentare der kommentierten Bilder beschreiben die Quantile $Q_{0,25} = 1$, $Q_{0,5} = 3$, $Q_{0,75} = 5$, $Q_{0,95} = 14$. 29,4 % aller Fotos hatten einen Bildtitel, der weder leer war noch mit einer gängigen Bilddateinamenserweiterung (GIF/JPG/PNG) endete, was auftritt, wenn Upload-Werkzeuge den Dateinamen als Standardwert für den Bildtitel setzen.

Die Statistik für einen Nutzer, die diesem als Ergebnis der Auswertung präsentiert wurde, enthielt 17 Angaben aus der Sicht des einzelnen Nutzers (vgl. Abbildung 5.16). Abbildung 5.17 zeigt die Häufigkeitsverteilung der individuellen Ergebnisse der wichtigsten 9 dieser 17 Werte: Die Anzahl der Fotos des Nutzers selbst und die Anzahl der Fotos seiner Freunde (genauer: nur jene, welche für eine App, die er nutzt, sichtbar sind), die Anzahl der zu den Fotos gehörenden Ortsangaben und Personen-Markierungen, Markierungen seiner selbst in eigenen Fotos und denen von Freunden sowie die Zahl der Fotos mit Ortsangaben, auf denen der Nutzer markiert ist. Die langen Rattenschwänze der Grafiken wurden für eine bessere Visualisierung abgeschnitten. Das persönliche Ergebnis eines Nutzers enthielt des Weiteren jeweils für die eigenen und für Freundesfotos die Anzahl verschiedener Ortsangaben und verschiedener markierter Personen, die Anzahl von Kommentaren und die durchschnittliche Anzahl von Kommentaren je Bild.

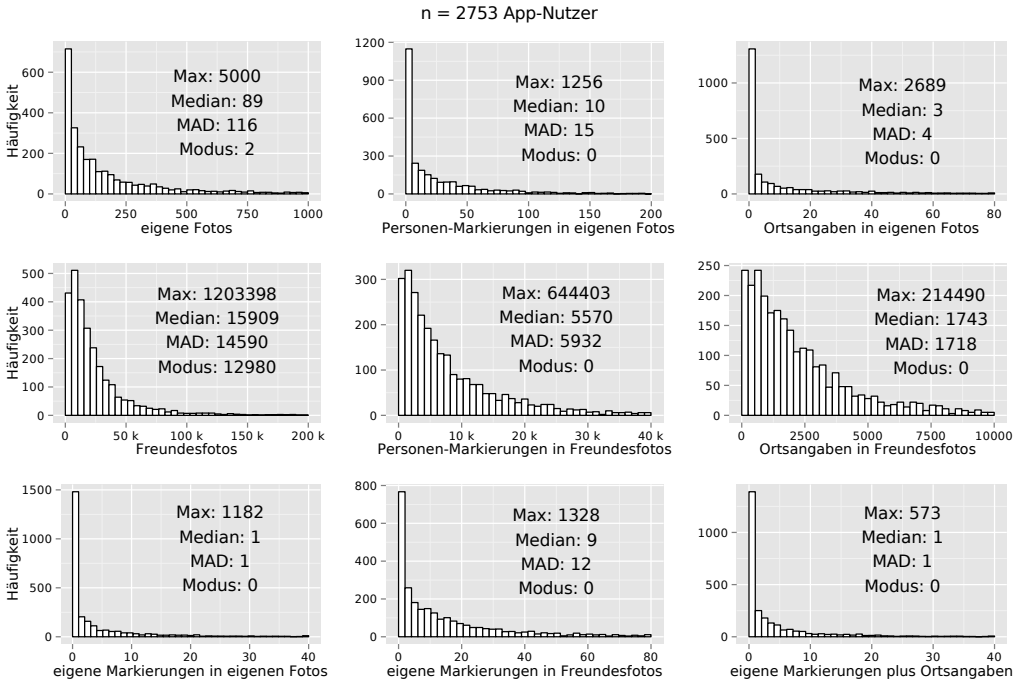


Abbildung 5.17: Häufigkeitsverteilung von Fotos, Ortsangaben und Personen-Markierungen in eigenen Fotos und Fotos direkter Freunde je Nutzer der Facebook-App Foto-Privatsphäre-Statistik

5.4.4.1 Zugriffsrechte für „Von anderen Nutzern verwendete Apps“

Facebook-Nutzer können eine Privatsphäre-Einstellung vornehmen, die den Namen „Von anderen Nutzern verwendete Apps“ trägt. Diese ermöglicht den Nutzern, zu unterbinden, dass von ihren Freunden genutzte Apps auf ihre persönlichen Daten, wie Fotos oder Profilinformationen, zugreifen können. Aus der Sicht einer App – wie auch aus Sicht der Foto-Privatsphäre-Statistik – hat ein Freund, der diese Option für Fotos aktiviert hat, keine Fotos. Die Antwort der Facebook-API kann in diesem Fall nicht von solch einer unterschieden werden, die zurückgegeben wird, wenn ein Freund wirklich gar keine Fotos teilt. Es ist jedoch relativ selten, dass jemand gar kein Foto teilt, da auch Foto-Beiträge in der eigenen Chronik und Profilbilder zu diesen zählen. Während diverser Testläufe der App konnte im Falle, dass die Facebook-API keine Fotos zurückgibt, jedes Mal verifiziert werden, dass der betrachtete Nutzer die unterbindende Einstellung aktiviert hatte. Natürlich gibt es auch Nutzer, die wirklich gar kein Foto bei Facebook teilen, jedoch ist zu vermuten, dass in den meisten Fällen die Privatsphäre-Einstellung der wahre Grund für die Auskunft über keine Fotos ist. Aus diesem Grund kann das Teilen keiner Fotos als Indikator für die Privatsphäre-Einstellung angenommen werden. Unter dieser Annahme wäre somit die Zahl der geteilten Fotos beachtlich höher, da rund 30 % der Freunde der App-Nutzer keine Fotos mit der App teilten. Nimmt man die 75,7 Millionen Fotos als repräsentative Stichprobe an, so hat die Privatsphäre-Einstellung keine Auswirkung auf die zuvor beschriebenen Anteile von Metadaten. Ein Einfluss auf die folgenden Vergleiche von Schätz- und Realwerten der Fotos kann hingegen angenommen werden, da die gemessenen Realwerte wohl geringer als die tatsächlichen Realwerte sind.

Der Median des Anteils von Freunden, welche keine Fotos teilten, unterscheidet sich zwischen den drei zuvor klassifizierten Nutzergruppen: Der Median der initialen Nutzer ist 35,1 %, der Median der DRadiohörer ist 32,7 % und der der Bildleser ist 26,2 %. Die Unterschiede zwischen der Gruppe der Bildleser und den anderen beiden Gruppen sind statistisch signifikant (Kruskal-Wallis-Test: $\chi^2_2 = 68$, $p < 0{,}001$; paarweise Wilcoxon-Mann-Whitney-Tests: initiale Nutzer versus DRadiohörer $z = 0{,}75$, $p = 0{,}45$; initiale Nutzer versus Bildleser $z = -6{,}7$, $p < 0{,}001$; DRadiohörer versus Bildleser $z = 5{,}04$, $p < 0{,}001$).

5.4.4.2 Entfernen der App und ihrer Berechtigungen

Auf der Willkommensseite der Facebook-App sowie in der Ergebnisbenachrichtigung via E-Mail wurden die Nutzer der App darauf hingewiesen, dass sie die App und damit die Zugriffsrechte auf ihre persönlichen Daten nach dem Erhalt der Ergebnisbenachrichtigung entfernen können, da die Ergebnisanzeige unabhängig von der Facebook-App war. Als über zwei Wochen nach der Nutzung der App durch die 2.753 Nutzer getestet wurde, ob diese die App entfernt hatten und ihr damit die Rech-

te entzogen hatten, war der Zugriff auf die Daten von 89,1 % der Nutzer weiterhin möglich. Trotz des deutlichen Hinweises hatte ein Großteil der Nutzer den Zugriff auf ihre persönlichen Daten nicht unterbunden. Dabei konnte ein deutlicher Unterschied im Verhalten der beschriebenen drei Nutzergruppen festgestellt werden: 92,9 % der Gruppe der initialen Nutzer, die hauptsächlich aus Studierenden und Universitätsmitarbeitern bestand, hatten der App die Rechte entzogen. 16,5 % der DRadiohörer-Gruppe hatten die Zugriffsrechte entfernt und nur 7,1 % der Gruppe der Bildleser, die vorwiegend über Bild Online auf die App gestoßen wurden, hatten dies getan. Die Unterschiede zwischen den Gruppen sind statistisch signifikant (Pearsons Chi-Quadrat-Test: initiale Nutzer versus DRadiohörer $\chi^2_1 = 111$, $p < 0{,}001$; initiale Nutzer versus Bildleser $\chi^2_1 = 8{,}4$, $p < 0{,}004$; DRadiohörer versus Bildleser $\chi^2_1 = 819$, $p < 0{,}001$).

5.4.5 Vergleich von Schätzungen und realen Werten

Im Folgenden werden für die 2.245 App-Nutzer, die den Pre-Fragebogen ausgefüllt haben, die abgegebenen Schätzungen mit den ermittelten Realwerten verglichen. Die demographische Zusammensetzung dieser App-Nutzer ist quasi identisch mit der aller App-Nutzer. Für einen besseren Überblick über die ermittelten Zahlen werden in diesem Abschnitt einige Werte nicht nur auf den aktuellen Kontext bezogen beschrieben, sondern auch auf die Menge aller 2.245 schätzenden App-Nutzer bezogen (aller Nutzer, abgekürzt als a. N.).

5.4.5.1 Fotos von Freunden

Die App-Nutzer wurden im Pre-Fragebogen nach ihrer Einschätzung gefragt, wie viele Fotos aller ihrer Facebook-Freunde sie insgesamt ansehen können, d. h. auf wie viele Fotos dieser sie Zugriff haben. Als mögliche Antworten waren vorgegeben: *keine Angabe* (Vorauswahl), *keine Vorstellung*, *unter 50*, *50*, die Zahlenwerte beschrieben durch $d \cdot 10^k, d \in \{1,\ldots,9\}, k \in \{2,\ldots,5\}$, *1.000.000*, und *über 1 Millionen*. 77,1 % der 2.245 Nutzer gaben eine Schätzung ab, 22,4 % antworteten mit *keine Vorstellung* und 0,5 % von ihnen beantworteten diese Teilfrage nicht. Am häufigsten schätzten sie die Zahl der Fotos, die all ihre Freunde teilen, auf 1.000. Dies entspricht auch dem Median der Schätzungen. Die übrigen Quartile der Schätzungen waren $Q_{0{,}25} = 400$, $Q_{0{,}75} = 8.000$. Der Median der realen Anzahlen geteilter Fotos war 15.909 ($Q_{0{,}25} = 7.722$, $Q_{0{,}75} = 30.687$) und das Maximum betrug 1.203.398. Abbildung 5.18 trägt die Häufigkeitsverteilung der Schätzungen und Realwerte gegeneinander auf.

Es stellt sich nun die Frage, wie viele App-Nutzer die Zahl der von ihren Freunden geteilten Fotos korrekt geschätzt haben. Nehme man dazu folgendes Maß für die Korrektheit an: Eine Schätzung wird als korrekt angesehen, wenn der Realwert näher am Schätzwert ist als an dessen Vorgänger oder Nachfolger aus der Menge

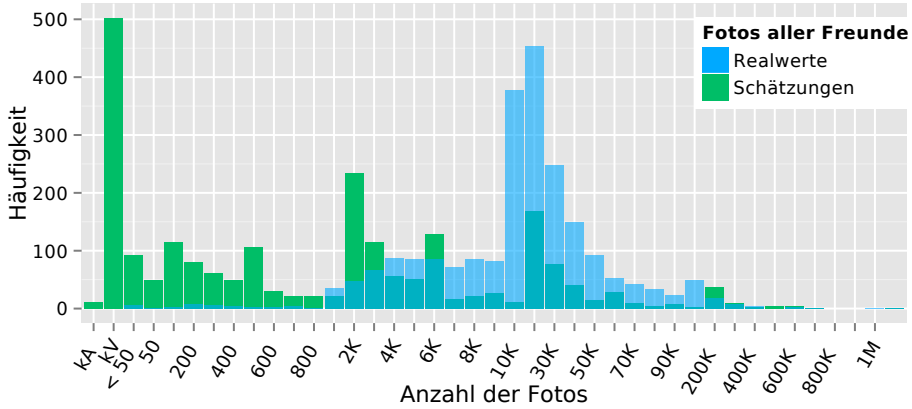


Abbildung 5.18: Schätzungen und reale Anzahl der Fotos von Freunden

der möglichen Antworten. So wäre beispielsweise die Schätzung 1.000 korrekt für die realen Werte im Intervall (950 : 1.500]. Wendet man dieses Maß zur Beurteilung an, so haben nur 3,9 % der Nutzer die Zahl der Fotos korrekt geschätzt, während 96,1 % nicht korrekt geschätzt haben. Dieses Maß deckt das Intervall der realen Werte vollständig ab. Er vermeidet Überlappungen der Intervalle und ist recht streng. Im Fragebogen wurde jedoch das genaue Verständnis der vorgegebenen Werte im Sinne von „mindestens“ oder „bis zu“ nicht genauer erläutert, um den Nutzern die Beantwortung zu vereinfachen. Dieses räumte den Nutzern jedoch auch einen gewissen Interpretationsspielraum ein. Um dies zu berücksichtigten, wird im Folgenden ein lockereres Maß verwendet, bei dem die Intervallgrenzen bis zum Vorgänger und Nachfolger einer Zahl reichen. Somit ist beispielsweise die Schätzung 1.000 korrekt für die realen Werte im Intervall (900 : 2.000]. Dies berücksichtigt die möglichen impliziten Interpretationen der Nutzer. Wendet man dieses Maß auf die Daten an, so waren 8,2 % der Schätzung korrekt im Sinne des gewählten Maßes (6,3 % a. N.), während 91,8 % der Schätzungen nicht korrekt waren.

Als Nächstes stellt sich die Frage, wie stark sich die Schätzung der übrigen 70,8 % aller App-Nutzer (1.590 Personen) von den realen Werten unterscheidet. Da der Vergleich der Häufigkeitsverteilungen wie in Abbildung 5.18 dargestellt keine Schlüsse über den Fehler der einzelnen Schätzungen zulässt, wird die Fehleinschätzung als Differenz der Schätzwerte und der Realwerte berechnet. Dies führt zu folgender Feststellung: 8,6 % der Nutzer, die eine Fehleinschätzung abgaben, haben die Zahl der Fotos von Freunden überschätzt (6,1 % a. N.). 91,4 % von ihnen unterschätzten die Zahl der Fotos, die ihre Freunde mit ihnen/ihrer App teilen (64,7 % a. N.). Abbildung 5.19 zeigt die Häufigkeitsverteilung aller Fehleinschätzungen. Um die absolute Fehlschätzung exemplarisch zu visualisieren, zeigt Abbildung 5.20 eine zufällige Stichprobe von 100 Schätzungen der Nutzer mit den Realwerten als Fehlerbalken.

Um weiter den Faktor der Fehlschätzung zu beurteilen, werden Schätzwert und Realwert dividiert. Dabei wird immer der größere Wert durch den kleineren geteilt,

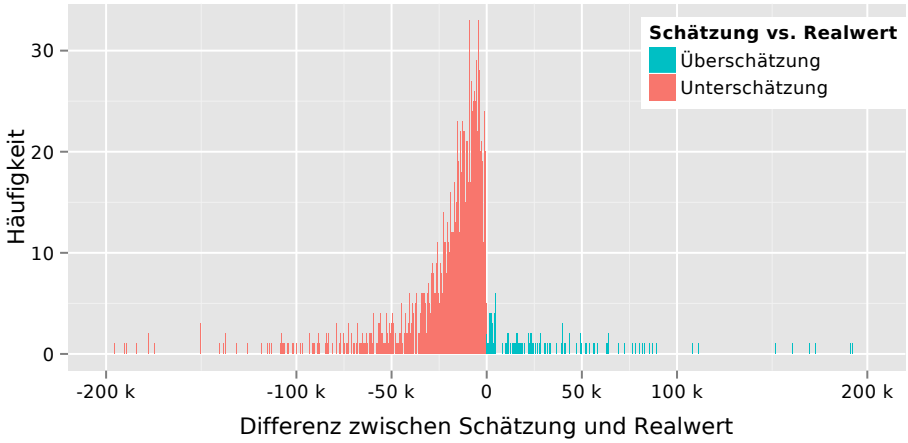


Abbildung 5.19: Häufigkeitsverteilung der Fehlschätzungen von Freundesfotos

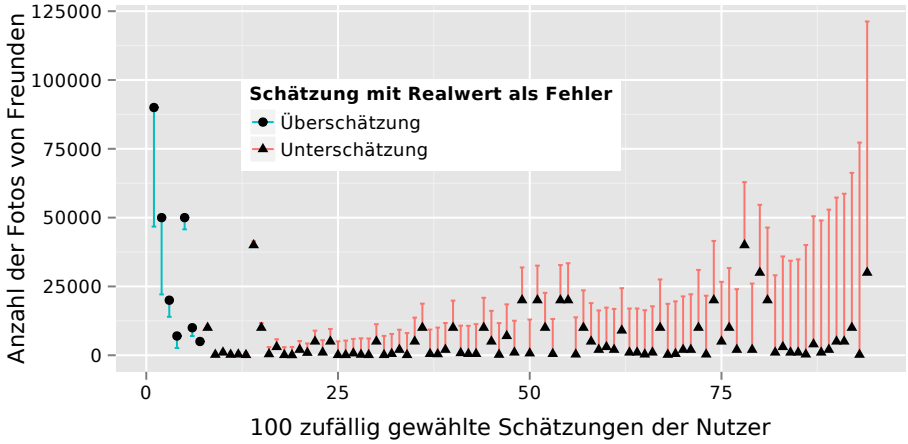


Abbildung 5.20: Zufällige Stichprobe (n = 100) aus 1.732 Schätzungen der Fotos von Freunden verglichen mit dem Realwert (Fehlerbalken)

ein negatives Vorzeichen steht für eine Unterschätzung und ein positives Vorzeichen für eine Überschätzung. Die Antwort *unter 50* wird als 25 kodiert, was dem Durchschnitt aller möglichen Realwerte entspricht. In Fällen der Antwort *über 1 Millionen* wird der Wert 1.000.001 verwendet. Der Faktor der Fehlschätzung ist über das Intervall von -38.989 bis 258 verteilt ($Q_{0,05} = -312$, $Q_{0,95} = 2$). Der Median der Fehlschätzung ist eine Unterschätzung um den Faktor -11 ($Q_{0,25} = -38$, $Q_{0,75} = -3$). Aufbauend auf dem Faktor der Fehlschätzung kann die dezimale Größenordnung der Fehlschätzung berechnet werden. Abbildung 5.21 zeigt die Häufigkeitsverteilung der Größenordnungen. 91,9 % der Überschätzungen waren von der Größenordnung 1 (5,6 % a. N.) und 8,1 % der Überschätzungen waren von einer höheren Größenordnung (0,5 % a. N.). Im Vergleich dazu wurden die meisten Unterschätzungen mit höherer Größenordnung gemacht: 43,7 % der Unterschätzungen waren von der Größenordnung 10 (28,3 % a. N.). 42 % von ihnen waren von der Größenordnung 1 (27,2 % a. N.). Weitere 13,1 % der Unterschätzungen waren von der Größenordnung

100 (8,5 % a. N.). Die übrigen 1,2 % waren von der Größenordnung 1.000 und 10.000 (0,7 % a. N.). Berücksichtigt man auch die Nutzer, die im Sinne der vorherigen Festlegung korrekt geschätzt haben, so verändert sich nur die Häufigkeit der Schätzungen von der Größenordnung 1. Klassifiziert man diese als Unter- und Überschätzung, so waren 62 % von ihnen Unterschätzungen und 38 % von ihnen Überschätzungen. Abbildung 5.21 zeigt diese als graue Teilbalken.

Zusammenfassend lässt sich feststellen, dass nur ein begrenzter Teil der Nutzer die Zahl der Fotos, die ihre Freunde teilen, korrekt einschätzen konnte. Die meisten Nutzer unterschätzten die Anzahl der Fotos. Berücksichtigt man, dass zumindest ein gewisser Teil der 30 % der Freunde, die mit der App keine Fotos teilten, auch noch Fotos teilt, ist das Ausmaß der Unterschätzungen zudem höher als hier beschrieben. Bei der Untersuchung der vorliegenden Daten konnten weder bei den Facebook-Daten noch bei den Schätzungen signifikante Unterschiede zwischen den verschiedenen Nutzergruppen festgestellt werden. Im Pre-Fragebogen schätzten rund 6 % aller 2.245 Nutzer die Zahl der Fotos von Freunden so, dass sie eher der Zahl der eigenen Fotos entsprachen als der ihrer Freunde. Es konnte nicht verifiziert werden, ob dies ein Fehler der Nutzer oder ein Fehlverständnis der Fragestellung war, oder ob dies die wahre Überzeugung der Nutzer widerspiegelte.

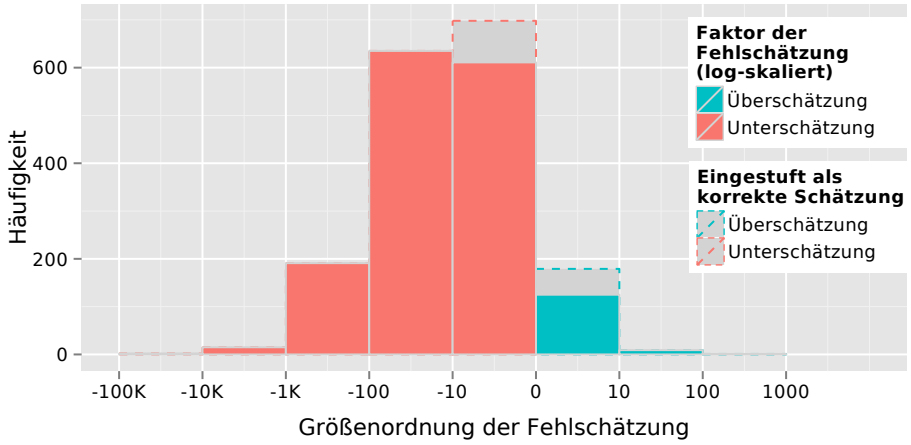


Abbildung 5.21: Häufigkeitsverteilung der Größenordnung der Fehlschätzung der Anzahl von Freudesfotos

5.4.5.2 Ortsangaben

Die App-Nutzer wurden im Pre-Fragebogen nach ihrer Einschätzung gefragt, wie viele Fotos ihrer Facebook-Freunde mit einer Ortsangabe versehen sind. Als mögliche Antworten waren vorgegeben: *keine Angabe* (Vorauswahl), *keine Vorstellung*, *keines*, *wenige* (< 10 %), *jedes zehnte* (10 %), *jedes fünfte* (20 %), *jedes dritte* (33 %), *jedes zweite* (50 %), *mehr* (> 50 %) und *jedes*. Die nicht äquidistanten Antworten wurden zugunsten der mehr intuitiven textuellen Formulierungen gewählt. 81,2 % der 2.245

Nutzer gaben eine Schätzung ab, 16,6 % antworteten mit *keine Vorstellung* und 2,2 % von ihnen beantworteten diese Teilfrage nicht.

Die Häufigkeiten der verschiedenen Antworten sind in Tabelle 5.4 dargestellt. Der Median der Schätzungen war, dass 20 % der Fotos eine Ortsangabe besitzen ($Q_{0,25} = 10\,\%$, $Q_{0,75} = 33\,\%$). Der Median der Realwerte war hingegen 10,8 % (MAD = 4 %, $Q_{0,25} = 8{,}4\,\%$, $Q_{0,75} = 13{,}9\,\%$). Nahezu unabhängig von den Schätzungen lagen die Realwerte zwischen 0 und 41,4 %. Gruppiert man die Nutzer gemäß ihrer Schätzwerte, so ist der Median der Realwerte der Gruppen nahezu identisch (10,5 % bis 10,7 %). Es existiert keine Tendenz, dass die Realwerte in Relation zu den jeweiligen Schätzwerten stehen. Diskretisiert man die Realwerte auf aufeinanderfolgenden Intervallen der Länge 5, so ist das häufigste auftretende Intervall in allen Gruppen das Intervall $[10; 15)$.

Schätzwert [% Fotos]	Anteil	Realwerte Intervall	Median	korrekt, wenn in	korrekt / alle	*MD*
0	0,4 %	(6,6; 12,3)	11,3	[0; 5]	0/7	-6,2
< 10	15,2 %	(1; 26,6)	10,5	[0; 10]	138/277	-3,8
10	23,4 %	(0; 35,8*)	10,5	[5; 15]	343/426	-2,5
20	23,9 %	(1; 40,3)	10,9	[15; 26,5]	84/436	5,0
33	19,1 %	(1; 41,4)	11,0	[26,5; 41,5]	3/349	15,5
50	9,8 %	(2; 38,1)	10,8	[41,5; 75]	0/178	30,7
> 50	7,7 %	(3; 26)	11,7	[50; 100]	0/140	38,3
100	0,5 %	(2,3; 26)	10,6	[75; 100]	0/9	64,4
alle	100 %	(0; 41,4*)	10,8	31,2 % korrekte Schätzungen		

* ein Ausreißer von 74,1 % wurde entfernt

Tabelle 5.4: Anteile und Korrektheit der Schätzwerte von Ortsangaben

Um zu entscheiden, ob eine Schätzung als korrekt angesehen wird, wurde folgendes Maß gewählt: Eine Schätzung gilt als korrekt, wenn der gerundete Realwert näher am gewählten Schätzwert liegt als an dessen vorbestimmten Nachbarwerten. Im Fall der als Intervall vordefinierten Antworten gilt die Schätzung als korrekt, wenn der Realwert im jeweiligen Intervall liegt. Tabelle 5.4 enthält die entstehenden Korrektheitsintervalle, in denen ein Realwert liegen müsste. Sie zeigt außerdem die Anteile der als korrekt klassifizierten Antworten. Die Spalte *MD* enthält den Median der Distanz zwischen Realwerten und den Korrektheitsintervallen. Wird das festgelegte Maß für die Bestimmung korrekter Schätzungen angewendet, so werden 31,2 % der Schätzungen als korrekt klassifiziert (25,3 % a. N.).

Um die Größe der Fehlschätzung der übrigen 55,9 % aller Nutzer (1.253 Personen) zu bestimmen, wird die Differenz zwischen Schätzwert und Realwert berechnet. Nur 17,8 % der Fehlschätzungen (10 % a. N.) waren Unterschätzungen der Menge an Fotos mit Ortsmarkierungen. Die übrigen 82,2 % der Fehlschätzungen (45,9 % a. N.) waren Überschätzungen. Abbildung 5.22 zeigt die Häufigkeitsverteilung der Fehlschätzungen. Sie zeigt ebenfalls die Abweichungen der als korrekt eingestuften

Schätzungen (58 % Unterschätzungen und 42 % Überschätzungen).

Es zeigt sich, dass die Nutzer den Anteil an Fotos mit Ortsangaben besser einschätzen können, als die Zahl der geteilten Fotos. Die meisten überschätzten den Anteil, während sie die Zahl der Fotos hingegen unterschätzten.

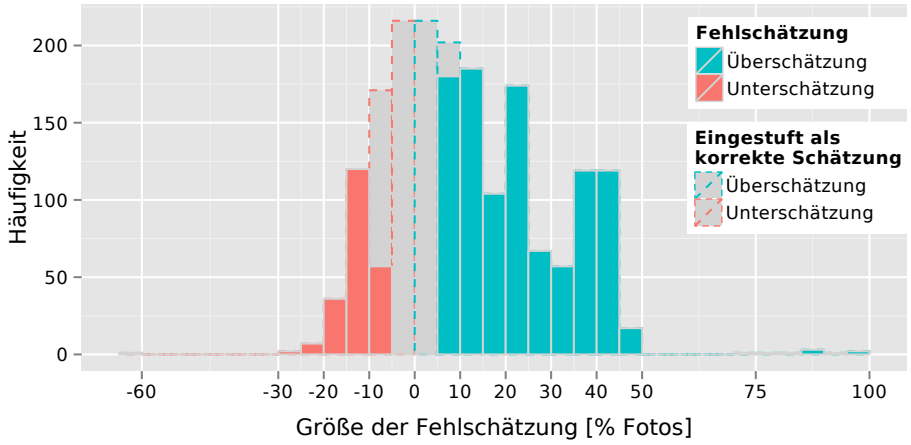


Abbildung 5.22: Häufigkeitsverteilung der Fehlschätzungen von Fotos mit Ortsangaben

5.4.5.3 Personen-Markierungen

Die App-Nutzer wurden im Pre-Fragebogen nach ihrer Einschätzung gefragt, wie viele Fotos ihrer Facebook-Freunde mit Personen-Markierungen versehen sind. Es standen dieselben vorgegebenen Antworten wie bei der vorherigen Frage zur Auswahl. 83,3 % der 2.245 Nutzer gaben eine Schätzung ab, 13,9 % antworteten mit *keine Vorstellung* und 2,8 % von ihnen beantworteten diese Teilfrage nicht.

Die Häufigkeiten der verschiedenen Antworten sind in Tabelle 5.5 dargestellt. Der Median der Schätzungen war, dass auf jedem dritten Foto (33 %) Personen markiert sind ($Q_{0,25} = 10\,\%$, $Q_{0,75} = 50\,\%$). Der Median der Realwerte war hingegen 17,8 % (MAD = 6,9 %, $Q_{0,25} = 13{,}5\,\%$, $Q_{0,75} = 22{,}7\,\%$). Die Realwerte waren über das Intervall von 0 bis 47,5 % gestreut. Gruppiert man die Nutzer gemäß ihrer Schätzwerte, so steigt der Median der gruppierten Realwerte mit den Schätzwerten von 10,2 % bis auf 22,6 %. Es existiert eine Tendenz, dass die Realwerte im Mittel in Relation zu den jeweiligen Schätzwerten stehen. Diskretisiert man die Realwerte auf aufeinanderfolgenden Intervallen der Länge 5, so steigen die Grenzen des häufigsten Intervalls i_{modus} mit den Schätzwerten: einmal $[5; 10)$, zweimal $[10; 15)$, dreimal $[15; 20)$ und zweimal $[20; 25)$.

Entsprechend der identischen vorgegebenen Antworten wurde bei dieser Frage auch dasselbe Maß für die Korrektheit der Schätzungen angewandt. Tabelle 5.4 enthält die verwendeten Korrektheitsintervalle, die Anteile der als korrekt klassifizierten Antworten und die Mediane der Distanz zwischen Realwerten und den Korrektheitsintervallen. Im Fall der Personen-Markierungen waren nur 23,3 % der Schätzungen

Schätzwert [% Fotos]	Anteil	Realwerte Intervall	Median	korrekt, wenn in	korrekt / alle	*MD*	i_{modus}
0	0,5 %	(4,4; 21,3)	11,2	[0; 5]	1/10	-8,1	[5; 10)
< 10	11,0 %	(0; 42,7)	14,3	[0; 10]	42/206	-5,8	[10; 15)
10	14,0 %	(3,2; 32,2)	15,2	[5; 15]	131/262	-4,7	[10; 15)
20	19,5 %	(2,2; 36,9)	16,5	[15; 26,5]	215/363	2,6	[15; 20)
33	20,3 %	(4,2; 36,8)	18,6	[26,5; 41,5]	44/380	8,9	[15; 20)
50	16,8 %	(3,4; 47,5]	19,4	[41,5; 75]	3/313	22,2	[15; 20)
> 50	17,0 %	(8,7; 44,2)	21,8	[50; 100]	0/318	28,2	[20; 25)
100	0,9 %	(8,3; 28,9)	22,6	[75; 100]	0/17	52,4	[20; 25)
alle	100 %	(0; 47,5)	17,9	23,3 % korrekte Schätzungen			

Tabelle 5.5: Anteile und Korrektheit der Schätzwerte von Personen-Markierungen

gemäß des gewählten Maßes korrekt (19,4 % a. N.). Die Ergebnisse lassen jedoch vermuten, dass die Schätzungen der Anzahl von Fotos mit Personen-Markierungen fundierter sind als im Fall der Ortsangaben. Es existiert ein Trend, dass in diesem Fall die Realwerte stärker mit den Schätzungen korrespondieren, wie die Betrachtung der Mediane der Realwerte und der Modi der in Intervalle diskretisierten Realwerte innerhalb der Gruppen gleicher Schätzung zeigt. Untersucht man Schätzwerte und Realwerte auf eine Korrelation, so zeigt Spearmans Rho ($\rho = 0{,}316$, $p < 0{,}01$) ebenfalls eine leichte Tendenz. Dies ist ein interessantes Ergebnis. Es wirft die Frage auf, wieso die Nutzer diese Informationen besser einschätzen können.

Um die Größe der Fehlschätzung der 63,9 % Nutzer (1.433 Personen), deren Schätzung als nicht korrekt klassifiziert wurde, zu bestimmen, wird die Differenz zwischen Schätzwert und Realwert berechnet. Nur 22,5 % der Fehlschätzungen (14,4 % a. N.) waren Unterschätzungen der Menge an Fotos mit Personen-Markierungen. Die übrigen 77,5 % der Fehlschätzungen (49,5 % a. N.) waren Überschätzungen. Abbildung 5.23 zeigt die Häufigkeitsverteilung der Fehlschätzungen. Sie zeigt ebenfalls die Abweichungen der als korrekt eingestuften Schätzungen (54,1 % Unterschätzungen und 45,9 % Überschätzungen). Wie im Fall der Ortsangaben tendieren die Nutzer dazu, den Anteil der Fotos mit Personen-Markierungen zu überschätzen.

Anzahl von Personen-Markierungen in einem Bild Die App-Nutzer wurden im Pre-Fragebogen zudem nach ihrer Einschätzung gefragt, wie viele Personen durchschnittlich auf einem Foto mit Personen-Markierungen markiert sind. Als mögliche Antworten waren vorgegeben: *keine Angabe* (Vorauswahl), *keine Vorstellung*, die Zahlen von 1 bis 10 und *mehr*. 78 % der 2.245 Nutzer gaben eine Schätzung ab, 18 % antworteten mit *keine Vorstellung* und 4 % von ihnen beantworteten diese Teilfrage nicht.

Der Median der Schätzungen war, dass ein Foto mit Personen-Markierungen drei solcher Markierungen enthält ($\varnothing = 2{,}8$). Die Antworten waren wie folgt verteilt: 7,5 % der Schätzungen gaben an, dass in Bildern mit Personen-Markierungen durch-

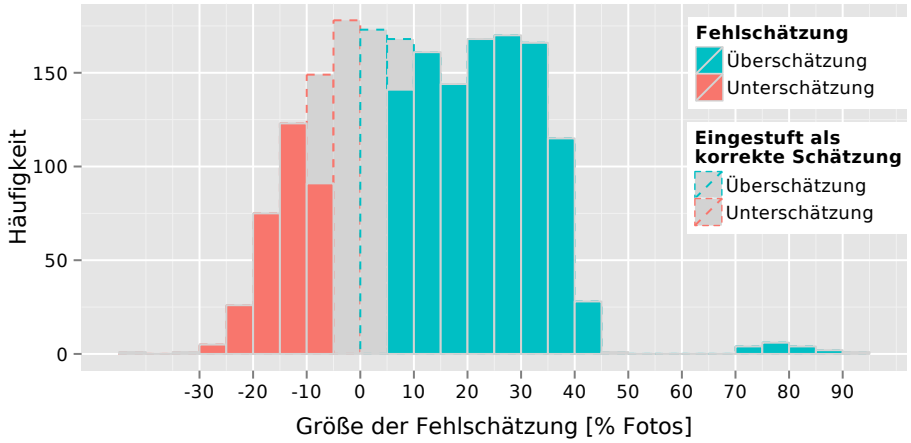


Abbildung 5.23: Häufigkeitsverteilung der Fehlschätzungen von Fotos mit Personen-Markierungen

schnittlich eine Person markiert ist. 39,3 % schätzten zwei Personen und 35,5 % gaben die Zahl drei an. 8 % der Schätzungen gaben vier Personen als Mittelwert an, 4,9 % von ihnen fünf, 3,6 % schätzten zwischen sechs und zehn Personen-Markierungen pro Bild und 1,2 % der Schätzungen gaben an, dass mehr als zehn Personen durchschnittlich in einem Bild mit Personen-Markierungen markiert sind. Der Median und der Durchschnitt der Realwerte war zwei. Die gerundeten Durchschnittswerte der Realwerte waren wie folgt verteilt: 1 % der Nutzer hatte Zugriff auf Fotos von Freunden mit Personen-Markierungen mit im Mittel einer Personen-Markierung. Bei 93,4 % der schätzenden Nutzer waren im Mittel zwei Personen auf solch einem Bild markiert. Bei 4,6 % der Nutzer waren es mit Mittel drei, bei 0,5 % von ihnen waren es vier, bei 0,2 % der Nutzer waren es im Mittel fünf und bei weiteren 0,2 % waren es im Mittel zwischen fünf und zehn Markierungen.

Keiner der Nutzer, die *mehr* als 10 Markierungen schätzten, schätzte dies korrekt. Sie überschätzten die durchschnittliche Anzahl von Personen-Markierungen auf Fotos mit Markierungen. Das Maximum der realen durchschnittlichen Anzahl an Personen-Markierungen auf Fotos von Freunden dieser Nutzer war 4,6. Betrachtet man die übrigen Schätzungen und vergleicht die Schätzwerte mit den gerundeten realen Durchschnittswerten, so waren 39,6 % der Schätzungen (30,6 % a. N.) korrekt. Bei 43,2 % der Schätzungen (33,4 % a. N.) lagen die Schätzwerte nur um eine Person neben den gerundeten realen Durchschnittswerten. Klassifiziert man die Größe der Fehlschätzung durch die Bildung der Differenz von Schätzwerten und gerundeten realen Durchschnittswerten (für die Antworten *1* bis *10* Personen-Markierungen), so stellen sich 15,5 % der Fehlschätzungen als Unterschätzung (7,2 % a. N.) und 84,4 % als Überschätzungen (39,3 % a. N.) dar. Abbildung 5.24 zeigt die Häufigkeitsverteilung der Fehlschätzungen aller Antworten. Für die Antworten von *mehr als 10* wurde dort für die Differenzbildung der Wert 11 verwendet.

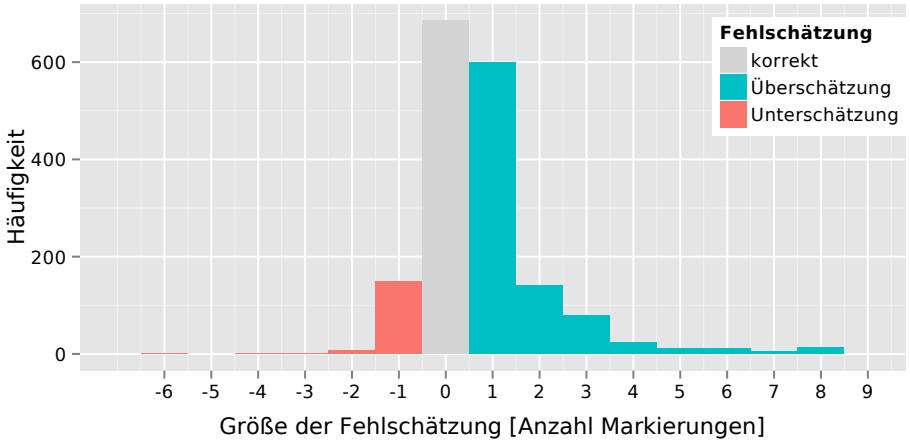


Abbildung 5.24: Häufigkeitsverteilung der Fehlschätzungen der durchschnittlichen Anzahl von Personen-Markierungen in Fotos mit Personen-Markierungen

5.4.6 Bewertung der App-Ergebnisse durch die Nutzer

Im Post-Fragebogen wurden die Nutzer um eine Bewertung ihrer persönlichen Foto-Privatsphäre-Statistik gebeten. Zwischen der Benachrichtigung über das Vorliegen der eigenen Ergebnisse und dem Ausfüllen des Fragebogens lagen im Mittel 5 Stunden ($Q_{0,75} \approx 14\,\text{Stunden}$, $Q_{0,95} \approx 2\,\text{Tage}$). Das Maximum der Zeitspanne waren 20 Tage. Die ursprünglichen eigenen Schätzungen wurden den Teilnehmern des Post-Fragebogens nicht nochmals gezeigt.

Die Teilnehmer wurden gefragt, ob sie solche Zahlen, wie ihre persönliche Statistik zeigte, zu den Fotos ihrer Freunde erwartet hätten. Es wurde eine 7-Punkte-Skala von *viel geringer als erwartet* über *wie erwartet* bis *viel höher als erwartet* verwendet. Abbildung 5.25 zeigt die Antworten der 269 Teilnehmer. Die Teilantworten unterscheiden sich statistisch signifikant (Friedman-Test: $\chi^2_3 = 31{,}88$, $p < 0{,}001$).

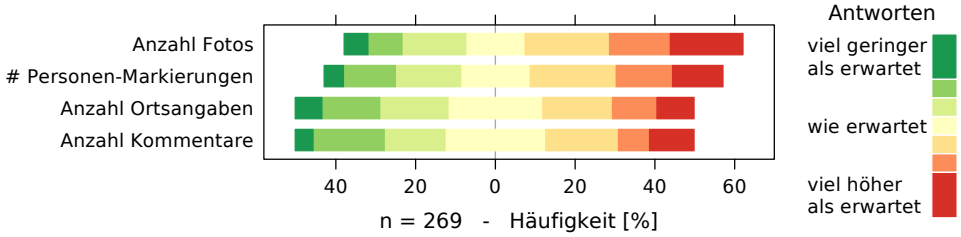


Abbildung 5.25: Bewertung der persönlichen Foto-Privatsphäre-Statistiken

Im Fall der Fotos, die ihre Freunde teilen, gaben 53,6 % der Teilnehmer an, dass die Zahl höher als erwartet war. 30,7 % von ihnen gaben an, dass die Zahl niedriger als erwartet war und 15,7 % meinten sie seien genau wie erwartet gewesen. Von den 214 der 269 Teilnehmer, welche anfangs auch eine Schätzung der Zahl der Fotos ihrer Freunde abgegeben hatten, gaben 59,3 % konsistente Antworten (weniger als erwartet, während sie überschätzten; mehr als erwartet, während sie unterschätzten). Die

Antworten von 25,7 % der Teilnehmer waren hingegen inkonsistent. Die übrigen 15 % hatten mit *wie erwartet* geantwortet. Die Schätzungen von 12,5 % der Letzteren waren als korrekt eingestuft worden. 59,4 % hatten sich um den Faktor 10 verschätzt und 28,1 % hatten eine Fehlschätzung bis zum Faktor 850 abgegeben. Diese Frage des Post-Fragebogens wurde auch von Teilnehmern beantwortet, die anfangs keine Schätzung abgegeben hatten. Deren Antworten werden zur Veranschaulichung separat in Tabelle 5.6 aufgeschlüsselt.

geschätzter Wert	Fotos		Ortsangaben		Personen-Mark.	
Antwort	*k.V.*	*k.A.*	*k.V.*	*k.A.*	*k.V.*	*k.A.*
Anzahl	34	21	25	22	18	25
niedriger als [%]	32,4	33,4	40,0	31,8	72,2	36,0
wie erwartet [%]	20,6	19,0	32,0	45,5	11,1	12,0
höher als [%]	47,0	47,6	28,0	22,7	16,7	52,0

k.V. = keine Vorstellung *k.A. = keine Angabe*

Tabelle 5.6: Beurteilung der persönlichen App-Ergebnisse durch die App-Nutzer, die anfangs nicht geschätzt hatten

Im Fall der Ortsangaben zu Fotos ihrer Freunde gaben 39,1 % der Teilnehmer an, dass die Zahl höher als erwartet war. 39,1 % von ihnen gaben an, dass die Zahl niedriger als erwartet war und 21,8 % meinten sie seien wie erwartet gewesen. Von den 226 Teilnehmern, die anfangs auch eine Schätzung abgegeben hatten, gaben 46 % konsistente Antworten. Die Antworten von 33,3 % der Teilnehmer waren inkonsistent in Bezug auf die anfängliche Schätzung. Die übrigen 20,7 % hatten mit *wie erwartet* geantwortet. 30,4 % letzterer schätzten korrekt im Sinne des definierten Maßes. Bei 28,3 % jener Teilnehmer unterschied sich der Realwert um bis zu 10 % vom Korrektheitsintervall. Bei den Übrigen war die Differenz größer.

Im Fall der Personen-Markierungen auf Fotos von Freunden gaben 47,6 % der Teilnehmer an, dass die Zahl höher als erwartet war. 34,3 % von ihnen gaben an, dass die Zahl niedriger als erwartet war und 18,1 % meinten sie seien wie erwartet gewesen. Eine Prüfung auf Konsistenz ist hier nicht möglich, da die zwei anfänglichen Fragen, die gewählt wurden, um das Schätzen einfacher zu gestalten, mit der einen im Post-Fragebogen nicht zu vergleichen sind.

Insgesamt gaben nur 6 Teilnehmer durchweg inkonsistente Antworten, jedoch gaben auch nur 27 Teilnehmer durchweg konsistente Antworten.

Im Post-Fragebogen wurden die Teilnehmer auch gefragt, wie sie über die wirklichen Zahlen auf der 7-Punkte-Skala von *sehr erschüttert* bis *sehr begeistert* empfinden. Wie Abbildung 5.26 zeigt, gaben mit 56,9 % mehr als die Hälfte der Teilnehmer an, diesem neutral gegenüberzustehen. 27,4 % gaben an, negativ über die Ergebnisse gestimmt zu sein und 15,7 % gaben an sie positiv zu empfinden.

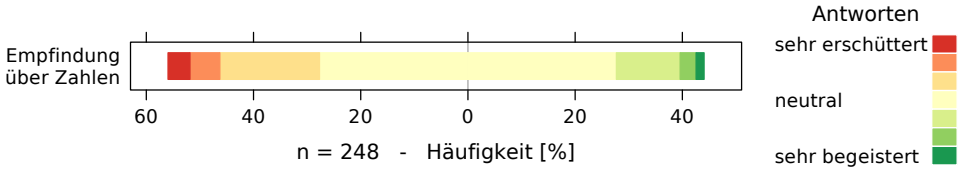


Abbildung 5.26: Empfindung über die realen Zahlen geteilter Fotos und Metadaten

5.4.7 Bewusstseins über geteilte Fotos im Allgemeinen

Im zweiten Teil des Post-Fragebogens wurde die Wahrnehmung der Nutzer über ihr Bewusstsein über geteilte Fotos im Allgemeinen erfasst. Um die Ergebnisse der in Abschnitt 5.3 beschriebenen Online-Umfrage zu verifizieren, wurden Teile aus dieser wiederholt. Es sollte untersucht werden, ob es Unterschiede zwischen den Teilnehmern der Online-Umfrage und den Teilnehmern dieser Studie gab, da Letztere einen sichergestellten Bezug zur Praxis hatten und durch ihre persönliche Statistik Indizien zum Ausmaß möglicher Bedrohungen kannten. Außerdem wurde der zuvor genannte positive Effekt von Personen-Markierungen mit Benachrichtigungen im Pre-Fragebogen nochmals betrachtet.

Vorhandenes Bewusstsein Die Teilnehmer wurden gefragt, wie gut sie sich über Fotos überall im Web informiert fühlen, auf denen sie zu sehen sind. Ihre Antworten konnten sie auf der 7-Punkte-Skala von *(1) völlig ausreichend* bis *(7) äußerst ungenügend* geben. Abbildung 5.27 zeigt ihre Antworten. Im Fall von schönen und angenehmen Fotos tendierte das angegebene Informationsniveau der Teilnehmer im Durschnitt dazu, leicht ungenügend zu sein ($\varnothing = 4{,}6$, $s = 1{,}9$, Median $= 5$, Modus $= 7$). 56 % von ihnen wählten eine Antwort schlechter als neutral und nur 6 % der Teilnehmer gaben an, dass das Informationsniveau *völlig ausreichend* sei. Im Vergleich dazu war das durchschnittlich wahrgenommene Informationsniveau im Fall von unerwünschten Fotos deutlich ungenügend ($\varnothing = 5{,}2$, $s = 1{,}8$, Median $= 6$, Modus $= 7$). Während nur 4 % mit den vorhandenen Informationen völlig zufrieden waren, gaben 70 % der Teilnehmer an, dass das Informationsniveau schlechter als neutral bis *völlig ungenügend* sei. Die Antworten auf beide Teilfragen unterschieden sich statistisch signifikant (Wilcoxon-Test: $z = -6{,}64$, $p < 0{,}001$). Im Vergleich zur vorherigen Online-Umfrage gaben die Teilnehmer dieser Studie an, sich weitaus schlechter informiert zu fühlen. Weniger als die Hälfte ($^6/_{22}, ^4/_{11}$) von ihnen gab an, sich *völlig ausreichend* informiert zu fühlen, während bis zu doppelt so viele ($^{56}/_{25}, ^{70}/_{39}$) angaben, ungenügend informiert zu sein.

Wahrnehmung von Personen-Markierungen Die Ergebnisse der Online-Umfrage in Abschnitt 5.3 haben gezeigt, dass Personen-Markierungen mit automatischer Benachrichtigung der am häufigsten genannte Weg war, um von Fotos seiner selbst zu

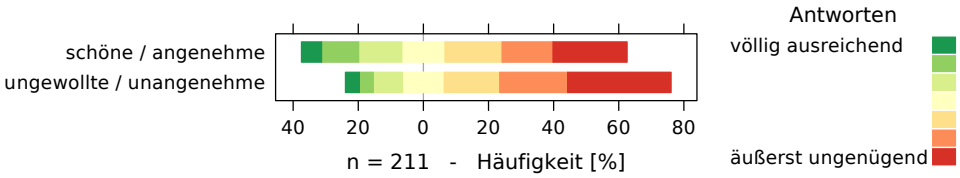


Abbildung 5.27: Wahrgenommenes Informationsniveau über sämtliche Fotos im Web, die die Studienteilnehmer zeigen

erfahren. Dies führt zu der Hypothese, dass Personen-Markierungen nicht nur als Bedrohung der Privatsphäre gesehen werden können, sondern auch als Hilfe zum Schutz der eigenen Privatsphäre, indem man den beschriebenen positiven Effekt nutzt. Um diese Hypothese zu evaluieren, wurden die Teilnehmer des Pre-Fragebogens gefragt, ob sie es als Privatsphäre-Vorteil wahrnehmen, auf Fotos markiert zu werden. Auf der 7-Punkte-Skala von *(1) nein – es ist eine große Bedrohung meiner Privatsphäre* bis *(7) ja – es birgt schlagkräftige Vorteile für meine Privatsphäre* mit *(4) neutral* gaben 15,4 % der 2.013 der App-Nutzer an, einen Vorteil für die Privatsphäre zu sehen, wie Abbildung 5.28 zeigt. Während 28,9 % von ihnen die Antwort *neutral* wählten, gaben 55,6 % von ihnen an, die Markierungen als Bedrohung für ihre Privatsphäre zu sehen (Median = 3, MAD = 1,5), wobei 43,2 % auf die schlechtesten zwei Antworten entfielen. Es muss festgestellt werden, dass obwohl die automatischen Benachrichtigungen infolge von Personen-Markierungen momentan der beste Weg zu sein scheinen über ein Foto seiner selbst informiert zu werden, mit 15,4 % nur relativ wenige Teilnehmer der Hypothese einer Hilfe zum Schutz der eigenen Privatsphäre zustimmen. Die Gründe dafür sollten in weiteren Arbeiten ergründet werden.

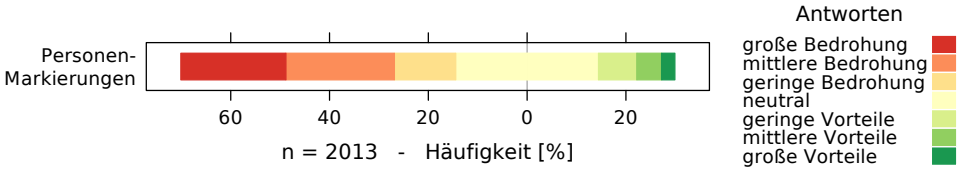


Abbildung 5.28: Wahrnehmung des Effekts von Personen-Markierungen mit Profilverknüpfung: Bedrohung oder Privatsphäre-Vorteil

Um die Wahrnehmung der Personen-Markierungen weiter zu evaluieren, wurden die Teilnehmer des Post-Fragebogens gebeten, die verschiedenen Effekte von Personen-Markierungen zu bewerten. Auf der 7-Punkte-Skala von *(1) gefällt mir sehr* über *(4) neutral* bis *(7) gefällt mir gar nicht* bestätigten die Antworten der 194 Facebook-Nutzer das Ergebnis der Online-Umfrage. Abbildung 5.29 fasst ihre Antworten zusammen. Von Fotos seiner selbst zu erfahren beziehungsweise Fotos von sich selbst zu finden wird im Durchschnitt weder besonders begrüßt noch besonders abgelehnt ($\varnothing = 4{,}0$, $s = 1{,}6$). Die meisten Teilnehmer bevorzugen, Fotos von Anderen zu finden ($\varnothing = 3{,}5$, $s = 1{,}6$) statistischer signifikant (Wilcoxon-Test:

$z = -3{,}56$, $p < 0{,}001$). Dies stützt das Ergebnis, dass die Teilnehmer keinen großen Privatsphäre-Vorteil in den Markierungen sehen. Die Teilnehmer gaben an, es eher nicht zu mögen, dass andere Fotos von ihnen finden können ($\varnothing = 4{,}7$, $s = 1{,}7$).

Die Teilnehmer, die dazu tendierten, es nicht zu mögen, dass Fotos von ihnen gefunden werden können, waren im Mittel seltener in ihren eigenen Fotos und in den Fotos ihrer Freunde markiert. Es konnte jedoch keine deutliche Korrelation für diese Teilmenge der Teilnehmer gezeigt werden: $n = 100$, $\rho_{\text{eigene}} = -0{,}22$, $\rho_{\text{Freunde}} = -0{,}38$, $p < 0{,}01$.

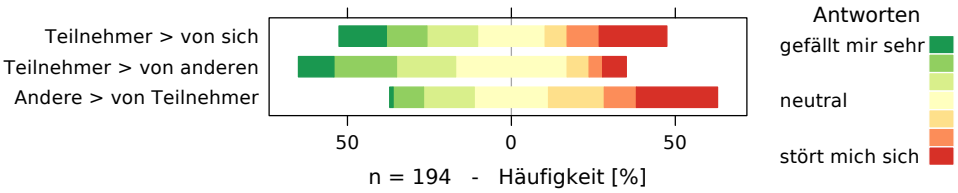


Abbildung 5.29: Wahrnehmung des Effekts von Personen-Markierungen mit Profilverknüpfung: Wer findet Fotos von wem

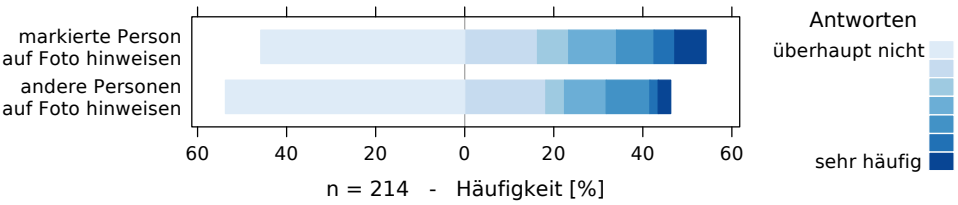


Abbildung 5.30: Gründe für das Markieren von Personen auf Fotos

Gründe für Personen-Markierungen Die Teilnehmer wurden außerdem gebeten auf der 7-Punkte-Skala von *(1) überhaupt nicht* bis *(7) sehr häufig* anzugeben, wie häufig sie andere Personen aus folgenden Gründen markieren. Abbildung 5.30 zeigt die Antworten der 214 Teilnehmer. 46 % der Teilnehmer gaben an, niemals jemanden zu markieren, nur um ihn auf ein Foto hinzuweisen. Die übrigen 54 % bewerteten diesen Grund mit einem durchschnittlichen Wert von 4 ($s = 1{,}8$), wobei 11 % auf die zwei häufigsten Antworten entfielen. 54 % der Teilnehmer gaben an, niemals jemanden zu markieren, nur um andere Personen auf das Foto des Markierten hinzuweisen. Die übrigen 46 % bewerteten diesen Grund mit einem durchschnittlichen Wert von 3,6 ($s = 1{,}8$), wobei 5 % auf die zwei häufigsten Antworten entfielen. Die Antworten auf beide Fragen unterschieden sich statistisch signifikant (Wilcoxon-Test: $z = -3{,}11$, $p < 0{,}001$). Die Ergebnisse zum Aufmerksammachen anderer sind quasi identisch mit den Ergebnissen der Online-Umfrage. Hingegen gaben deutlich weniger Teilnehmer an, aus Bewusstmach-Gründen Personen zu markieren: 46 % antworteten mit *überhaupt nicht*, während in der Online-Umfrage nur 30 % Vergleichbares antworteten. Der Durchschnitt der Antworten war im Post-Fragebogen 4, während er in der Online-Frage bei 5,34 lag.

5.4.8 Diskussion

Dieser Abschnitt diskutiert die wichtigen Ergebnisse der Studie.

5.4.8.1 Demographie

Die ungleichmäßige Verteilung des Geschlechts der App-Nutzer ist sehr wahrscheinlich auf die Teilnehmer-Rekrutierung zurückzuführen. 93 % der Nutzer entstammen der Gruppe der Bildleser. Die Leserschaft von *Bild Online* hat eine Verteilung der Geschlechter von 60 % männlich zu 40 % weiblich. Es kann unterstellt werden, dass die Verschiebung zu noch mehr männlichen Nutzern daher rührt, dass der Nutzer gewinnende Artikel im Resort Internet auf `Bild.de` erschienen ist.

Weder in den Ergebnissen der persönlichen Statistiken noch in den Beantwortungen der Fragebögen konnten signifikante Unterschiede zwischen männlichen und weiblichen Nutzern gefunden werden. Es konnten ebenfalls keine signifikanten Unterschiede bei einer Gruppierung nach Alter oder den (häufigsten) Herkunftsländern gefunden werden. Ein Grund hierfür könnte sein, dass das Geschlecht eines Nutzers, sein Alter oder Herkunftsland einen wohl eher geringen Einfluss darauf hat, was seine Freunde teilen und markieren. Die demographischen Angaben dieser Personen konnten nicht erfasst und somit auch nicht bei der Analyse berücksichtigt werden.

5.4.8.2 Ausmaß der Fotos und Metadaten je Nutzer

Immer wieder geben Berichte durch Aussagen wie „mehr als 350 Million Fotos werden durchschnittlich pro Tag bei Facebook hochgeladen“ [61] einer Vielzahl interessierter Nutzer einen teils schwer vorstellbaren Eindruck, wie viele Inhalte insgesamt im Social Web geteilt werden. Sie geben den Nutzern jedoch erst recht keinen Eindruck über das Ausmaß von Fotos in ihrem persönlichen Umfeld. Die im Rahmen der Studie verwendete Facebook-App tut einen ersten Schritt in diese Richtung, indem sie Bewusstsein über das Ausmaß der Fotos schafft, die im direkten Bekanntenkreis durch die direkten Facebook-Freunde geteilt werden. Im Gegensatz zu Zahlen aus allgemeinen Berichten über Dienste des Social Webs mögen die persönlichen Zahlen den einzelnen Nutzer mehr berühren und ihm das Ausmaß geteilter Fotos greifbarer und eindringlicher darstellen. Die Zahl der Fotos war in den persönlichen Foto-Statistiken häufig schon enorm hoch, wenn nur die Fotos der direkten Bekannten betrachtet worden sind. Viele Dienste des Social Webs erlauben hingegen den Zugriff aus Fotos von Bekannten höherer Bekanntschaftsgrade, wie *Freunde von Freunden* oder das öffentliche Teilen von Inhalten.

Abbildung 5.17 gab einen groben Überblick über das Ausmaß der Daten, die für einen einzelnen Nutzer sichtbar sind. Der durchschnittliche Nutzer der Facebook-App hatte zum Zeitpunkt der Datenerhebung Zugriff auf 16.000 Fotos seiner direkten

Facebook-Freunde. Diese Fotos hatten im Mittel über 5.500 Personen-Markierungen, 1.700 Ortsangaben und 21.900 Kommentare. Diese Menge an Daten ist damit schon weitaus höher als das, was ein einzelner Nutzer manuell begutachten könnte.

5.4.8.3 Bedrohung durch Apps

Betrachtet man mögliche Bedrohungen und Schäden für die Privatsphäre durch Facebook-Apps, so zeigt der erhobene Datensatz deutlich, wie schnell das Ausmaß von Daten, auf die eine App zugreifen kann, wächst. Nimmt man die relativ geringe Zahl von 2.753 Nutzers der präsentierten Facebook-App, so haben diese Nutzer der App den Zugriff auf mindestens 75,7 Millionen Fotos gewährt, in denen 6,3 Millionen verschiedene Personen markiert waren. Folglich könnte schon eine App mit so einem geringen Verbreitungsgrad die Privatsphäre von über 6 Millionen Menschen bedrohen. Die Erhebung und Verwendung solcher Zahlen könnte im Vergleich zu diversen allgemeinen Statistiken sehr wertvoll für die Bildungsarbeit und Aufklärung zum Thema Privatsphäre sein.

Weniger als ein Drittel aller Freunde der App-Nutzer verweigerten Apps von anderen Nutzern den Zugriff auf ihre geteilten Bilder. Es ist nicht ersichtlich, wie viele dieser solch eine Restriktion der Zugriffsrechte nicht für notwendig erachten. Ebenso können sie gar nicht von der Einführung dieser Privatsphäre-Einstellung wissen. Aufgrund der Dimension der durch diese Einstellung entstehenden Bedrohung sollte dieser Aspekt noch weiter evaluiert werden.

5.4.8.4 Schätzungen und Unbewusstsein

Ein großer Teil der App-Nutzer war sich nicht über das Ausmaß der geteilten Fotos bewusst, wie Tabelle 5.7 zusammenfassend zeigt. Die meisten der 2.245 App-Nutzer, die im Pre-Fragebogen Schätzungen abgaben, waren nicht fähig die Zahl der Fotos, die ihre Freunde teilen, angemessen zu schätzen. Nur 6,3 % schätzten die Zahl der Fotos korrekt ein. 22,4 % der Teilnehmer gaben an, dass sie *keine Vorstellung* über die Zahl der geteilten Fotos hätten. 64,7 % von ihnen unterschätzten die Zahl der Fotos ihrer Freunde, wobei mehr als die Hälfte der Unterschätzungen (37,5 % a. N.) mit einem Faktor größer 10 abgegeben wurden. Die Teilnehmer unterschätzten das Ausmaß der Fotos um einen beträchtlichen Faktor. Selbst wenn man Fehlschätzungen von der dezimalen Größenordnung von 1 noch als akzeptabel ansieht, haben immer noch 39 % der Teilnehmer des Pre-Fragebogens erhebliche Fehlschätzungen abgegeben. Abschließend lässt sich nur feststellen, dass die meisten Menschen sich nicht über das Ausmaß potenziell bedrohlicher Fotos bewusst zu sein scheinen. Es darf hier nicht vergessen werden, dass die Facebook-App nur Fotos direkter Freunde berücksichtigte, so dass die erfassten Werte lediglich untere Schranken darstellen.

Im Fall der für Facebook typischen Metadaten waren die Nutzer der App fähig,

Daten	*keine Angabe*	*keine Vorstellung*	als korrekt eingestuft	Fehlschätzung Unterschätzung	Fehlschätzung Überschätzung
Anzahl Fotos	0,5	22,4	6,3	64,7 (+3,9)	6,1 (+2,4)
mit Ortsangaben	2,2	16,6	25,3	10 (+14,7)	45,9 (+10,6)
mit Personen-Mark.	2,8	13,9	19,4	14,4 (+10,5)	49,5 (+8,9)
∅ Personen-Mark.	4,0	18,0	30,6	7,2	40,2

Fehlschätzungen in Klammern sind jene als korrekt eingestufte Schätzungen

Tabelle 5.7: Zusammenfassung des Vergleichs von Schätzwerten und Realwerten

diese weitaus besser zu schätzen. 25,3 % der Teilnehmer schätzten den Anteil der Fotos mit Ortsangaben korrekt im Sinne des verwendeten Maßes und 19,4 % von ihnen schätzten den Anteil der Fotos mit Personen-Markierungen korrekt. Auch wenn der prozentuale Anteil geringer ist, schienen die Schätzungen im Fall von Personen-Markierungen fundierter zu sein, da die Schätzungen deutlich besser mit den Realwerten korrespondierten. 30,6 % der Teilnehmer schätzten die durchschnittliche Zahl der Personen-Markierungen auf Bildern mit solchen Markierungen exakt auf den Realwert. Wobei die geringere Auswahl an Möglichkeiten dabei auch zu einigen Glückstreffern geführt haben kann. Im Fall der Metadaten hat der überwiegende Teil der Teilnehmer die Werte überschätzt, während die Zahl der Fotos vorwiegend unterschätzt wurde. Facebook-Nutzer scheinen ein besseres Gefühl für den Anteil an Metadaten in geteilten Fotos zu haben als für die Zahl der Fotos selbst. Eventuell reicht die Stichprobe der Fotos in der *Chronik* eines Nutzers aus, um einen repräsentativen Einblick in die Verwendung von Metadaten in ihrem Bekanntenkreis zu bekommen. Hingegen werden viele Nutzer nicht alle Fotoalben ihrer Freunde durchstöbern. Selbst wenn die Chronik-Beiträge ihrer Freunde zeigen, wie teil-freudig diese im Vergleich untereinander sind, so gibt dies noch keinen Hinweis über das eigentliche Ausmaß der geteilten Bilder insgesamt. Abschließend muss festgehalten werden, dass auch wenn Überschätzungen aus Sicht des Privatsphäreschutzes besser als Unterschätzungen sind, jegliche Fehlschätzung als ein Zeichen fehlenden Bewusstseins gewertet werden sollte.

5.4.8.5 Inkonsistenz der Antworten

Für einen Teil der Antworten des Post-Fragebogens konnte festgestellt werden, dass diese konsistent zum Vergleich der Schätzwerte und Realwerte gegeben wurden. Ein erheblicher Teil der gegebenen Antworten war jedoch inkonsistent, beispielsweise wenn jemand die Zahl der Fotos unterschätzte und angab, dass das persönliche Ergebnis zu Fotos niedriger als erwartet war. Ein Grund hierfür mag die Zeit sein, welche zwischen dem Pre- und dem Post-Fragebogen verstrich. Die Inkonsistenzen können jedoch genauso als ein weiteres Zeichen für das fehlende Bewusstsein über das Ausmaß der geteilten Bilder und Metadaten gewertet werden. Da es für alle Teile

der Studie keinen weiteren Anreiz als das Interesse an den eigenen Zahlen und dem Thema selbst gab, können absichtliche Fehleingaben und rein zufällige Antworten zum größten Teil ausgeschlossen werden.

5.4.8.6 Bewusstsein der Nutzer im Allgemeinen

Die Ergebnisse des Post-Fragebogens bestätigten die Ergebnisse der Online-Umfrage in Abschnitt 5.3 und zeichneten zum Teil ein schlechteres Bild. Die Teilnehmer dieser Studie gaben an, sich noch schlechter über Fotos ihrer selbst im Web informiert zu fühlen. Die durchschnittliche Wahrnehmung der Wirkung von Personen-Markierungen war quasi identisch zur Online-Umfrage. Die Teilnehmer dieser Studie gaben an, Personen-Markierungen seltener zu verwenden, um eine markierte Person auf ein Bild hinzuweisen. Mit 15,4 % der Pre-Fragebogen-Teilnehmer sahen nur wenige Teilnehmer einen Vorteil für die eigene Privatsphäre in Personen-Markierungen. Somit hält die Hypothese des Privatsphäre-Vorteils nur sehr beschränkt.

Neben dem stärkeren Bezug zur Realität im Fall der Facebook-App kann ein weiterer Grund für die Differenzen zur Online-Umfrage der Unterschied der Populationen beider Studien sein. Die Online-Umfrage fand im universitären Umfeld statt. Ein großer Teil der App-Nutzer entstammt eventuell nicht diesem Umfeld.

Interessant ist die Beobachtung, dass auch wenn drei Viertel der Teilnehmer angaben, nicht ausreichend über Fotos im Web informiert zu sein, die meisten von ihnen angaben, nicht empört zu sein, sondern vorwiegend neutral über die Zahlen ihrer persönlichen Foto-Privatsphäre-Statistik zu empfinden.

5.4.9 Fazit

Das Unvermögen vieler Teilnehmer die Menge von Bildern und Metadaten innerhalb des Kreises ihrer direkten Facebook-Freunde annähernd schätzen zu können ist ein deutliches Zeichen für fehlendes Wissen über das Ausmaß geteilter Fotos. Die Ergebnisse der durchgeführten Studie weisen auf ein hohes Maß von fehlendem Bewusstsein über geteilte Fotos hin. Diese Erkenntnis, die zuvor nur auf Basis von Selbsteinschätzungen erfasst wurde, wurde durch diese Studie in Zahlen gefasst. Die Ergebnisse des Post-Fragebogens bestätigen außerdem einen Teil der Erkenntnisse der Online-Umfrage aus Abschnitt 5.3.

Auch wenn viele Teilnehmer des Post-Fragebogens der Menge geteilter Fotos im eigenen Bekanntenkreis eher neutral gegenüberstanden, ist es wichtig, den Nutzern einen Zugang zu entsprechenden Zahlen zu ermöglichen. Zahlen, wie die von der App *Foto-Privatsphäre-Statistik* bereitgestellten, ermöglichen es den Nutzern erst zu entscheiden, ob sie eine Bedrohung ihrer Privatsphäre sehen (wollen) oder nicht. Auch wenn ein Teil der Nutzer von den Zahlen unbeeindruckt bleibt, so ermöglichen

sie anderen einen realen Eindruck von ihrer Situation. Erst mit dem Wissen über ihre Situation können die Nutzer entscheiden, ob sie Schutzmaßnahmen nutzen wollen.

Die Ergebnisse der Studie unterstreichen die Notwendigkeit für Methoden zum Schutz der Privatsphäre, die es Nutzern erlauben von den jeweiligen Fotos zu erfahren, die ihre Privatsphäre betreffen könnten. Solche Methoden müssen über existierende Privatsphäre-Einstellungen und Zugriffskontrollmechanismen hinausgehen, da die hier herausgestellte Quelle der Bedrohung durch Inhalte anderer außerhalb des Einflussbereichs der Nutzer liegt. Die Nutzer müssen im Detail über das sie betreffende Ausmaß geteilter Fotos aufgeklärt werden, um auch anhand der Dimension möglicher Probleme fundierte Entscheidungen zum Schutz der eigenen Privatsphäre treffen zu können. Die hier verwendete Facebook-App geht einen ersten Schritt in diese Richtung. Während die meisten Nutzer nur allgemeine Statistiken über große Masse von Bildern kennen, ermöglicht sie einen Einblick in den global gesehen minimalen Teil der großen Massen, der für einen einzelnen Nutzer jedoch schon eine manuell nicht beherrschbare Herausforderung darstellt.

Während seiner Keynote bei der Konferenz *CHI 2014* ging Vint Cerf – „Chief Internet Evangelist“ bei Google und einer der „Väter des Internets“ – auf das Problem ein, dass geteilte Fotos auch dritte Personen im Hintergrund eines Bildes betreffen können. Er drang darauf, dass es eine Aufgabe der Forschung sei, den Menschen zu ermöglichen, mit den entwickelten Technologien vernünftig umzugehen und verständig zu handeln. Es ist zu vermuten, dass ein Teil der Nutzer die durch ihre geteilten Fotos eventuell verursachten Bedrohungen nicht sieht, nicht versteht oder nicht verstehen möchte. Während es durch technische Mittel direkt nicht möglich ist, die Nutzer zum Umdenken oder zur Veränderung ihres (Teil-)Verhaltens zu bewegen, so können technische Mittel dazu dienen den Nutzern Informationen und Werkzeuge an die Hand zu geben, damit sie von sich aus das Ausmaß der geteilten Bilder, ihres Teil-Verhaltens und möglicher Konsequenzen besser verstehen lernen. Auf diese Weise kann die von Cerf betonte Verantwortung der Forschung zu einem Teil wahrgenommen werden.

Die Nutzer müssen nicht nur befähigt werden, ihre eigenen Inhalte zu beherrschen, was bisher im Fokus der Forschung und Praxis stand. Sie müssen ebenso befähigt werden, von Inhalten anderer zu erfahren, die sie persönlich und ihre Privatsphäre betreffen könnten, um sich im Weiteren vor eventuell schädlichen Inhalten zu schützen. Zuletzt müssen die Nutzer – vielleicht letztendlich durch die eigene Bedrohung durch andere – auch realisieren, dass ihre Inhalte auch eine Auswirkung auf andere haben können.

5.5 Konzepte zur Unterstützung der aktiven Suche nach relevanten Bildern

Eine Möglichkeit sich gegen fremdverursachte Bedrohungen durch Fotos Anderer zu schützen, ist die aktive Suche nach bedrohlichen Bildern. Für die Nutzer ist es jedoch aufgrund der Masse an geteilten Fotos schier unmöglich, die Fotos, welche sie persönlich betreffen könnten, manuell zu handhaben. Vor allem aber ist es für sie kaum möglich, den für sie relevanten Teil der *Big Data* der Social Media zuvor ausfindig zu machen. Die im Folgenden beschriebenen Konzepte [135] könnten die Nutzer bei der Suche nach relevanten Bildern unterstützen, indem sie helfen, die Menge der zu prüfenden Bildern handhabbarer zu machen.

5.5.1 Design

In der Analyse von Metadaten geteilter Bilder in Abschnitt 5.2 wurde gezeigt, dass ein erheblicher Teil der geteilten Fotos Ortsinformationen enthält. Außerdem wurde gezeigt, dass der Anteil von Fotos mit Ortsangaben mit der Zeit gestiegen ist. Es ist zu vermuten, dass sich dieser Anstieg fortsetzt, da immer mehr Geräte, ob Digitalkameras oder Kamera-Handys, Techniken wie GPS, WLAN oder Bluetooth integrieren, die zur Ortsbestimmung verwendet werden können. Während Ortsinformationen bei den Nutzern auf der einen Seite große Besorgnis in Bezug auf ihre Privatsphäre auslösen, können diese Informationen auf der anderen Seite auch zum Schutz der Privatsphäre eingesetzt werden. Wenn ein Nutzer die Ortsbestimmungsfunktionen seines Mobiltelefons nutzt, um seine Wege und Aufenthaltsorte mit den dazugehörigen Zeiten aufzuzeichnen, kann durch den Abgleich der Ortsangaben geteilter Bildern mit seinen Aufzeichnungen die Menge der zu betrachtenden Bilder signifikant verringert werden.

Im Folgenden werden verschiedene auf diesem Gedanken aufbauende Konzepte zur Unterstützung der aktiven Suche nach relevanten Bildern vorgestellt. Sie bestehen jeweils aus einer Client- und einer Serverkomponente. Der Nutzer trägt und steuert die Client-Komponente, die seine Aufenthaltsorte lokal auf dem Gerät aufzeichnet. Durch die Konfiguration des Clients kann er bestimmen, wann sein Ort aufgezeichnet wird und wann nicht, abhängig davon, ob er die entsprechenden Orte oder Zeiträume als relevant für seine Privatsphäre ansieht. Der Client kann ein Smartphone mit einer entsprechenden App sein. Es könnte jedoch auch ein spezielles, gegen ungewollten Zugriff besonders geschütztes Gerät sein, welches beispielsweise auf heute verfügbaren GPS-Loggern aufbaut. Auf Basis der Bewegungsaufzeichnungen kann der Nutzer über den zugehörigen Server-Dienst fokussiert die Bilder betrachten, die in seiner Nähe entstanden sind und seine Privatsphäre betreffen könnten. Hierzu sendet der Client die Aufzeichnungen oder Ausschnitte aus diesen an den Server,

der dem Nutzer die zeitlich und örtlich dazu passenden Bilder zurückgibt.

Der Server-Dienst kann auf verschiedene Weise realisiert werden. Er kann einerseits durch den betrachteten Webdienst zum Teilen von Fotos oder das Soziale Onlinenetzwerk selbst (kurz: Fotodienst) oder durch einen Dritten angeboten werden. Wird der Suchdienst durch den Fotodienst angeboten, so hat dieser vollen Zugriff auf alle Fotos aller Nutzer. Zugriffsbeschränkungen müssen erst bei der Nutzerinteraktion und Visualisierung respektiert werden, wenn entschieden wird, ob eventuell betroffenen Nutzern ein Bild gezeigt werden darf. Bei solch einer integrierten Lösung müssten gegebenenfalls interne Strukturen und Funktionen so erweitert werden, dass eine Suche nach Bildern mit einer Einschränkung auf Orte/Gebiete und Zeiträume möglich ist. Ein Fotodienst selbst könnte einen Suchdienst sowohl als Basisfunktionen für alle seine Nutzer anbieten oder als kostenpflichtigen Mehrwertdienst. Wird der Suchdienst durch einen dritten Anbieter realisiert, so unterliegt schon die Suche selbst den vorhandenen Zugriffsbeschränkungen. Damit er die Suche umsetzen kann, muss der Suchdienst auf die Daten des Fotodienstes zugreifen können, was über entsprechende Programmierschnittstellen oder Web-Crawling möglich wäre. Finanzierungsmodelle für einen dritten Anbieter könnte ein Pay-Per-Use-Modell, ein Abonnement des Suchdienstes oder eine Finanzierung durch Werbung sein. Die Suche nach Fotos kann in beiden Fällen im Namen eines Nutzers oder anonym geschehen. Im Folgenden werden vier Varianten des Dienstes vorgestellt.

1. Fotodienst – nutzerbezogen In dieser Variante wird der Suchdienst vom Fotodienst selbst angeboten. Der Dienst agiert im Namen des jeweiligen Fotodienst-Nutzers und mit dessen Zugriffsberechtigungen. Da der Fotodienst vollen Zugriff auf alle Bilder aller Nutzer hat, kann die Menge aller öffentlich zugänglichen Fotos berücksichtigt werden. Zusätzlich werden die Bilder in Betracht gezogen, auf die der Nutzer außerdem Zugriff hat, wie beispielsweise private Fotos seiner Freunde. Durch den Zugriff auf die Fotos von Freunden und Bekannten eines Nutzers können die Bilder berücksichtigt werden, auf denen der Nutzer mit höherer Wahrscheinlichkeit zu sehen ist. Außerdem werden so die Bilder berücksichtigt, die auch den Personen zugänglich sind, die Bedrohungen der Privatsphäre des Nutzers mit einer höheren Wahrscheinlichkeit entstehen lassen könnten, da sie eine Verbindung zu ihm haben. Handelt es sich beim Fotodienst um ein Soziales Onlinenetzwerk und nicht nur um eine einfache Foto-Community, so besteht bei dieser Variante ein deutlicher Anreiz für den Betrieb in den Ortsinformationen der Nutzer. Diese sind für Soziale Onlinenetzwerke eine kostbare Information, die sie eventuell auch für das Angebot weiterer Funktionen verwenden können. Aus der Sicht eines Nutzers ist die Kehrseite der Suche in seinem Namen, dass der Dienst erfährt, wann und wo er sich aufgehalten hat, da es eine eindeutige Verbindung zwischen Nutzer und Ortsinformationen gibt. Hier kommen die Abwägungen zum Tragen, die in der Online-Umfrage in Abschnitt 5.3.5

betrachtet wurden. Mit Sicherheit gibt es Nutzer, die es nicht stört, dass ihr Soziales Onlinenetzwerk erfährt, wann sie wo gewesen sind, wenn sie im Gegenzug relevante Fotos besser ausfindig machen können. Ebenso sicher gibt es auch Nutzer, denen ihre Privatsphäre über alles geht und die solch einem Tausch nie zustimmen würden.

2. Fotodienst – anonym Alternativ kann der Suchdienst vom Fotodienst so angeboten werden, dass keine Verbindung zwischen Ortsinformationen und einem Nutzer hergestellt werden kann. In diesem Fall werden alle Suchen anonym durchgeführt. Folglich ist bei dieser Variante der Suchraum des Dienstes kleiner, da ausschließlich die öffentlichen Fotos berücksichtigt werden können. Ein weiterer Nachteil dieser Variante ist, dass der Ansporn für den Betreiber nutzerbezogene Ortsinformationen zu erhalten, nicht gegeben ist und er somit keinen Vorteil aus dem Angebot des Suchdienstes ziehen könnte, außer dem Wunsch der Nutzer nach der Privatsphäre-Schutzfunktion nachzukommen.

3. Dritter Anbieter – nutzerbezogen Neben dem Fotodienst selbst kann ein dritter Anbieter einen Suchdienst anbieten. Um Zugriff auf die Informationen des Fotodienstes zu erlangen, wird bei dieser Variante der Zugriff auf die Daten durch den jeweiligen Nutzer ermöglicht. Der Suchdienst wird autorisiert, im Namen des Nutzers zu handeln und Daten abzufragen. Diese Art von Integration als *App* geschieht heute oft im Rahmen von Diensten wie Facebook oder Flickr, um den Nutzern weitere Funktionen zu bieten. Für die Autorisierung bietet sich dabei OAuth als Technologie an, welches auch in den genannten Fällen verwendet wird. Die Möglichkeiten einer Implementierung durch einen Dritten ist von den vorhandenen Programmierschnittstellen des Fotodienstes abhängig. Dieser müsste die zuvor beschriebenen Suchfilter dem dritten Anbieter zur Verfügung stellen, um einen Suchdienst zu realisieren. Für eine Betrachtung aller öffentlichen Fotos müssten ebenfalls entsprechende Funktionen vorhanden sein. Sonst bleibt nur die Suche innerhalb der Fotos der direkten Bekannten, die auf der Kontaktliste eines Nutzers verzeichnet sind oder naher Bekannter, die auf andere Weise identifiziert werden. Auch bei dieser Variante bekommt der Fotodienst Ortsinformationen, die er einem Nutzer eindeutig zuweisen kann. Diese können auch hier als wertvolle Informationen für den Fotodienst angenommen werden. Ein besonderer Ansporn für den Fotodienst die Umsetzung einem dritten Anbieter zu überlassen und die dazu notwendigen Schnittstellen zu schaffen ist nicht gegeben, so dass diese Variante als wenig praxistauglich anzusehen ist.

4. Dritter Anbieter – anonym Wenn ein dritter Anbieter nicht im Namen eines Nutzers agiert und er sehr wahrscheinlich nicht auf speziell bereitgestellte Suchschnittstellen aufbauen kann, bleibt ihm nur auf existierende anonym verwendbare Programmierschnittstellen oder auf das klassische Crawlen der zugehörigen Webseiten zurückzugreifen. In diesem Fall agiert der Suchdienst wie eine Suchmaschine.

Er durchsucht öffentlich verfügbare Fotos des Fotodienstes und indexiert die Fotos mit zugehörigen Ortsangaben und Zeiten in seiner eigenen Datenbank. Suchanfragen von Nutzern werden ausschließlich auf dem selbst aufgebauten Datenbestand durchgeführt, für den auch die notwendigen Suchfilter umgesetzt werden können.

Die Umsetzung durch einen dritten Anbieter hat zum Vorteil, dass ein solcher als Mash-up-Dienst mehrere Fotodienste in Betracht ziehen könnte. In allen Fällen bleiben die privaten Fotos fremder Personen außen vor. Inwieweit öffentliche Fotos der Dienste berücksichtigt werden können, hängt vom jeweiligen Fotodienst ab. Während beispielsweise die Foto-Community Flickr API-Zugriff auf öffentliche Fotos oder Web-Crawling technisch auch für Dritte ermöglicht, könnte eine vollständige Berücksichtigung öffentlicher Bilder beispielsweise bei Facebook nur vom Sozialen Onlinenetzwerk selbst vorgenommen werden.

Alle Varianten unterstützen den Nutzer lediglich dabei, die Menge der zu betrachtenden Bilder auf ein eher handhabbares Maß herunter zu brechen. Sie helfen Bewusstsein über potenziell bedrohliche Fotos zu schaffen, welche jemand anderes unbedacht und ohne böswillige Absichten geteilt hat. Die Konzepte schützen nicht vor böswillig geteilten Fotos, die der Privatsphäre eines Nutzers absichtlich schaden sollen. Sie können solche Fotos auch finden, jedoch kann ein Suchdienst dieser Art mit dem entsprechenden Wissen über seine Funktionsweise so ausgetrickst werden, dass schadhafte Bilder von ihm aussortiert und dem Nutzer nicht präsentiert werden.

5.5.2 Privatsphäre-Bewertung

Die verschiedenen Varianten des Suchdienstes können die Nutzer beim Schutz ihrer Privatsphäre unterstützen, indem sie helfen, die Zahl der Fotos zu reduzieren, die ein Nutzer zur Wahrung einer Privatsphäre kontrollieren muss. Es muss jedoch auch bedacht werden, dass solch ein Dienst selbst Bedrohungen für die Privatsphäre verursachen kann, wenn er nicht korrekt umgesetzt wird. Die verwendeten persönlichen Informationen der Nutzer müssen so behandelt werden, dass die Anforderungen der Nutzer an die Funktion und an die Wahrung ihrer Privatsphäre erfüllt werden. Kritisch zu betrachten ist daher der Schutz der Ortsinformationen, die ein Nutzer an den Suchdienst übermittelt und die dieser gegebenenfalls an den Fotodienst weitergibt.

In allen Fällen müssen Ortsinformationen dem Suchdienst anvertraut werden. In den Fällen der nutzerbezogenen Suche kann eine mögliche Bedrohung der Privatsphäre durch die Preisgabe der Ortsinformationen an den Fotodienst nicht verhindert werden, da die Informationen für die Suche notwendig sind und die Verknüpfung mit dem Nutzer für den Gewinn zusätzlicher Suchtreffer verwendet wird. Eine Möglichkeit die Privatsphäre zu schützen, wäre die Verschleierung der Ortsinformationen. Die einzelnen Orte könnten auf verschiedene Weise ungenauer gemacht werden. Dies hätte aber zur Folge, dass die Suchergebnisse ebenso ungenau sind. Das Hinzufügen

von Rauschen würde den Umfang des Suchergebnisses stark vergrößern. Mehrere Suchanfragen mit zeitgleichen Bewegungsprofilen, von denen nur eines der wahren Bewegung entspricht, könnten an den Suchdienst übermittelt werden, so dass dieser nicht weiß, wo der Nutzer wirklich war. In diesem Fall würde der Nutzer nur die Antwort auf die korrekte Anfrage verwerten. Dies würde es dem Fotodienst erschweren, den wahren Ort des Nutzers zu erfahren, es jedoch nicht verhindern. Diese Art von Privatsphäreschutz skaliert aus zweierlei Gründen nicht: Es wird sehr viel unnötige Last für den Suchdienst und den Fotodienst erzeugt. Ebenso komplex ist die Erstellung von gefälschten Bewegungsprofilen, die nicht direkt als Fälschung erkannt werden. Hier müssen selbst Indizien, die auf den wahren Ort oder das wahre Bewegungsprofil schließen lassen, wie die IP-Adresse des Clients, berücksichtigt werden.

In den Fällen der anonymen Suche besteht keine Bedrohung durch die Bindung an einen Nutzer. Hier müssen die übrigen identifizierenden Merkmale wie Cookies oder Client-IP-Adressen durch entsprechende Anonymisierungstechniken, wie Web-Proxys oder das TOR-Netzwerk, geschützt werden, so dass ein Nutzer, der sowohl die Suchfunktion als auch den Fotodienst in kurzer Abfolge nutzt, nicht wiedererkannt werden kann. Die anonymen Bewegungsprofile könnten immer noch von den Diensten missbraucht werden, doch sind sie ohne eine Nutzerzuordnung weniger kritisch für den einzelnen Nutzer. Basiert die anonyme Suche auf einem der Finanzierungsmodelle, bei der ein Nutzer für die Leistung bezahlt, muss zusätzlich darauf geachtet werden, dass keine Verbindung zwischen den Kundendaten und den Suchanfragen entsteht oder missbraucht wird. Hier spielt besonders das Vertrauen in den Suchdienst-Anbieter eine große Rolle, wie auch bei anderen kommerziellen Anonymisierungsdiensten im Internet. Bei der Finanzierung durch Werbung spielen die Methoden zum Schutz vor Missbrauch von Cookies oder IP-Adressen eine Rolle.

Nicht zuletzt muss auch der Nutzer-Client, welcher die Ortsinformationen lokal sammelt, gegen Zugriff durch Fremde geschützt werden. Die Aufzeichnung der Ortsinformationen selbst kann zudem durch diverse Einflussmöglichkeiten wie Ausschlusslisten von Gebieten oder Zeiten, eingeschränkt werden, um von vornherein die Sammlung von Daten auf das Notwendigste zu beschränken.

5.6 Ein Dienst zur Benachrichtigung über relevante Bilder

Die im vorherigen Abschnitt beschriebenen Konzepte können die Nutzer bei der proaktiven Suche nach Bildern unterstützen. Sie wurden so konzipiert, dass sie mit nur geringfügigen Erweiterungen existierender Dienste als Zusatzangebot umgesetzt werden können. Nutzer müssen dabei regelmäßig ihre aufgezeichneten Bewegungsdaten aktiv in die Suche einspeisen, um von relevanten Fotos zu erfahren. Im Folgenden

wird ein Konzept präsentiert sich gegen fremdverursachte Bedrohungen zu schützen [108], das einer tieferen Integration in einen Fotodienst bedarf, dafür jedoch nur wenig aktive Beteiligung eines Nutzers benötigt, bis ein relevantes Foto hochgeladen wird und der Nutzer über dies informiert wird.

Der Dienst *SnapMe* baut verstärkt auf die in Abschnitt 5.3.5 evaluierten Privatsphäre-Kompromisse auf. Wie bei den Konzepten des vorherigen Abschnitts werden Ortsinformationen eines Nutzers für die Identifizierung relevanter Fotos verwendet. Außerdem helfen Methoden zur Gesichtserkennung die Ergebnisse zu verbessern. Das zugrunde liegende Konzept basiert auf zwei Annahmen:

1. Der Trend der Verwendung von Ortsinformationen als Metadaten geteilter Bilder setzt sich ähnlich fort wie bisher.
2. Die Verbreitung mobiler Geräte mit integrierten Ortsbestimmungsfunktionen setzt sich fort wie bisher oder steigt sogar.

SnapMe hilft den Nutzern von solchen Fotos zu erfahren, die ihre Privatsphäre potenziell bedrohen könnten. Das Hauptziel des Dienstes ist, Bewusstsein über Fotos zu schaffen, die ohne böswillige Absichten geteilt werden. Dies schließt die große Menge spontan und unüberlegt gemachter Schnappschüsse ein, die sowohl durch Freunde als auch durch fremde Personen in der Umgebung der Nutzer entstehen. Die Schaffung von Bewusstsein geschieht nach dem Best-Effort-Prinzip: SnapMe ist nicht fähig jedes für einen Nutzer relevante Foto im Web zu finden, jedoch ermöglicht der Dienst, das Bewusstsein der Nutzer zu verbessern und die Zahl potenziell bedrohlicher Fotos zu minimieren. Will jemand böswillig der Privatsphäre eines Nutzers schaden, indem er bloßstellende Fotos veröffentlicht, ist es möglich SnapMe zu umgehen. Auch wenn ein Teil dieser Bilder durch SnapMe entdeckt werden könnte, ist der Dienst nicht darauf ausgelegt, den Nutzer gegen aktive Angriffe auf seine Privatsphäre zu schützen. Der Dienst soll primär dem Schutz der Privatsphäre dienen, er kann jedoch auch zum Finden gewünschter Bilder eingesetzt werden, die ein Nutzer schön findet und deren Teilen und Erhalt der Nutzer begrüßt.

5.6.1 Design

Der SnapMe-Dienst wird in den regulären Prozess des Hochladens integriert. Dies ermöglicht die Bilder direkt zum Zeitpunkt des Hochladens zu untersuchen, so dass Nutzer möglichst zeitnah über sie informiert werden können, um die Gefahr einer Bedrohung oder eines Schadens zu minimieren. Des Weiteren können durch die Integration in das Hochladen Informationen für die Prüfung verwendet werden, ohne dass diese längerfristig gespeichert werden müssen. So können beispielsweise Ortsangaben ausschließlich zur Betroffenseinprüfung verwendet und danach verworfen werden. Die Implementierung im Kern des Fotodienstes erlaubt die Prüfung unabhängig

von Zugriffsbeschränkungen einzelner Nutzer durchzuführen, welche somit erst bei einer späteren Benachrichtigung von Betroffenen berücksichtigt werden müssen.

Abbildung 5.31 umreißt die Funktionsweise von SnapMe. Die mit einem R markierten Personen sind beim Fotodienst für die SnapMe-Funktion registriert. Wird ein Foto geschossen und beim entsprechenden Fotodienst hochgeladen, wird anhand der vorhandenen Informationen geprüft, welche Nutzer betroffen sein könnten. Diese werden daraufhin über das sie potenziell betreffende Foto in ihrer Nähe informiert. Wird allein auf Basis von räumlicher Nähe benachrichtigt, so wird der rote Nutzer 1 (falsch-positiv) informiert, auch wenn er auf diesem Foto nicht zu sehen ist. Der grüne Nutzer 2 wird informiert, ist auf dem Foto und kann je nach der Ausgestaltung seiner weiteren Möglichkeiten handeln. Der nicht registrierte blaue Nutzer 3 ist auf dem Foto abgebildet, er wird jedoch nicht darüber informiert.

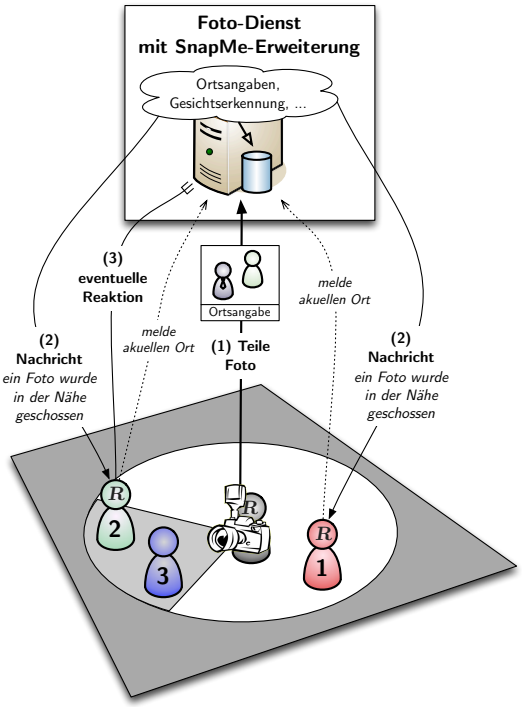


Abbildung 5.31: Grundlegende Funktionsweise des SnapMe-Dienstes zur Benachrichtigung von Nutzern über Fotos in ihrer Nähe

5.6.1.1 Geographische Kollokation

Als grundlegender Indikator, ob ein Foto für einen Nutzer relevant ist, wird die geographische Kollokation des Ortes, an dem das Bild entstanden ist – der Ort des Fotografen, und des Ortes des jeweils betrachteten Nutzers verwendet.

Die Ortsangabe eines Fotos (Koordinaten oder eine textuelle Ortsbeschreibung) kann durch einen Client in die Bilddatei eingebettet und auf diese Weise hochgeladen werden. In diesem Fall extrahiert SnapMe die Daten aus dem Foto. Alternativ kann

der Ort eines Fotos als Parameter beim Hochladen spezifiziert werden. In diesem Fall kann der Nutzer festlegen, ob der Ort ausschließlich durch den SnapMe-Dienst verwendet und danach verworfen wird, oder ob die Koordinaten als fotodienstinterne Metadaten für das Bild gespeichert werden sollen. Neben den Zeitangaben in den integrierten Metadaten wird der Zeitpunkt des Hochladens eines Bildes für die weiteren Prüfungen gespeichert.

SnapMe sieht zwei Möglichkeiten vor, den Ort des Nutzers zu spezifizieren. Der Nutzer kann *fixe private Orte* festlegen, die so behandelt werden, als sei der Nutzer immer an diesen. So kann sich der Nutzer über alle Fotos an diesen Orten direkt informieren lassen oder aber die Fotos zuvor weiteren Prüfungen unterziehen lassen. Ein solcher Ort wird durch die Angabe von Koordinaten und einem Kreisradius um den festgelegten Punkt bestimmt. Fixe private Orte erlauben es dem Nutzer, beispielsweise Fotos in der Nähe seiner Wohnung oder seiner Arbeitsstätte prüfen zu lassen. Durch die Angabe von Zeiten kann die Berücksichtigung des Ortes ausschließlich für eine bestimmte Zeitspanne einmalig oder auch wiederkehrend aktiviert werden. So können auch gezielte Ereignisse im Vorfeld unter Beobachtung gestellt werden. Alternativ kann der Nutzer einen standortbezogenen Dienst verwenden, um seinen *dynamischen privaten Ort* seinem eigenen Standort wie einen Schatten folgen zu lassen. Der dynamische private Ort wird somit durch die Koordinate des aktuellen Aufenthaltsortes bestimmt sowie durch einen Kreisradius, den jeder Nutzer individuell festlegen kann. Um den dynamischen Schutz nutzen zu können, installiert ein Nutzer beispielsweise die dazugehörige SnapMe-Client-App auf seinem Mobiltelefon. Will der Nutzer die Funktion nutzen, so aktiviert er die Bewegungsverfolgung in der App, welche daraufhin in regelmäßigen Zeitintervallen seinen aktuellen Aufenthaltsort an den SnapMe-Dienst sendet. Durch das Aktivieren und Deaktivieren des „privaten Schattens“ kann der Nutzer bestimmen, wann er die dynamische Kollokationsprüfung verwendet. Dies ermöglicht ihm, beispielsweise die Funktion nur bei speziellen Ereignissen zu nutzen. Für die grundlegende Bestimmung der geographischen Kollokation des dynamischen privaten Ortes wird der Ort eines Fotos jeweils mit der letzten Ortsangabe vor dem Zeitstempel eines Bildes und soweit möglich, mit der ersten Ortsangabe nach diesem verglichen. Da die Bewegung eines Nutzers zwischen diesen nicht bekannt ist, ist davon auszugehen, dass beispielsweise durch Interpolation keine besseren Ergebnisse erzielt werden können.

Verzögerung und Datenvorhaltung Um Bilder und Personen effektiv auf geographische Kollokation zu testen, muss die Prüfung eines Fotos für eine gewisse Zeitspanne ab dem Aufnahmezeitpunkt verzögert werden. Dies ermöglicht die Berücksichtigung dynamischer Ortsinformationen, welche zeitnah nach dem Erstellen eines Bildes gemeldet werden. Die zur Prüfung notwendigen Informationen müssen entsprechend für die Zeitspanne der Verzögerung vorgehalten werden. Das zeitweili-

ge Vorhalten der Ortsinformationen verbessert zudem die Erfolgsrate der Prüfung, da so auch die Zeitspanne berücksichtigt wird, die selbst bei spontan geteilten Bildern zwischen dem Erstellen eines Bildes und dem Hochladen liegt. Vergleicht man für die beiden Flickr-Datensätze *Flickr-50k-mobil-2012/-2013* aus Abschnitt 5.2 die Zeitstempel der Fotoerstellung mit denen des Hochladens, so lag bei 44,3 % der Fotos die dazwischen liegende Zeitspanne unter einer Stunde, bei 36,6 % unter einer halben Stunde und bei 29,2 % unter 15 Minuten. Es kann angenommen werden, dass beide Effekte für spontan geteilte Fotos mit einer Verzögerung zwischen 30 und 60 Minuten ausreichend berücksichtigt werden.

Kompassrichtung Immer mehr Kamerageräte integrieren neben Techniken zur Ortsbestimmung auch einen Kompass. Die Speicherung der Kompassrichtung einer Aufnahme wird von integrierten Metadaten unterstützt. Sie könnte auch als Parameter beim Hochladen übermittelt werden. Auf Basis der Kompassrichtung einer Aufnahme kann die Menge der Personen, für die ein Bild relevant ist, bei der Kollokation genauer bestimmt werden.

5.6.1.2 Gesichtserkennung

Die geographische Kollokation ist ein gutes Mittel die Zahl der relevanten Fotos zu reduzieren. Jedoch gibt es Situationen, in denen auf diese Weise trotzdem eine kaum oder auch gar nicht handhabbare Menge an Fotos als relevant für einen Nutzer eingestuft wird, die dieser im Folgenden manuell prüfen müsste. Beispielsweise bei Festivals, Demonstrationen oder anderen Großveranstaltungen kann dies selbst mit einem kleinen Radius für den dynamischen privaten Ort geschehen.

In diesen Fällen kann die Verwendung von Gesichtserkennung die Zahl relevanter Fotos weiter verringern oder Gesichtserkennung kann dazu eingesetzt werden, die zu prüfenden Fotos für die manuelle Sichtung zu bewerten und vorzusortieren. Abbildung 5.32 zeigt wie die Kollokationsprüfung und Gesichtserkennung bei der Prüfung von Bildern miteinander verbunden werden können. Wird ein Foto mit Ortsinformationen hochgeladen, so dass es von SnapMe weiter geprüft werden kann, wird die Gesichtserkennung verwendet, um Gesichter auf dem Bild zu detektieren. Werden keine Gesichter auf einem Bild gefunden, so kann es für die gesamte Prüfung verworfen werden oder es wird nur auf Kollokation getestet. Hat ein Nutzer für sich die Funktion zur Gesichtserkennung aktiviert und Vergleichsbilder bereitgestellt, so wird für ein durch Kollokation als relevant bestimmtes Bild geprüft, ob der Nutzer auf diesem wiedererkannt werden kann. So kann er sich nur über die Bilder informieren lassen, auf denen er auch zu erkennen ist.

Neben der Preisgabe des aktuellen Standortes stellt die Bereitstellung von Vergleichsbildern zum Trainieren der Gesichtserkennung für SnapMe einen weiteren

Privatsphäre-Kompromiss dar. Soziale Onlinenetzwerke haben in vielen Fällen schon hinreichend viele Vergleichsbilder für eine große Zahl ihrer Nutzer. Einige von ihnen nutzen diese auch schon für Vorschläge von Personen-Markierungen auf Basis von Gesichtserkennung. Inwieweit die Nutzer willens sind, diese Informationen zum Finden relevanter Bilder nutzen zu lassen, wurde in Abschnitt 5.3.5 anfänglich betrachtet. Hier existiert Potenzial für weitere Forschungsarbeiten, beispielsweise im Rahmen einer prototypbasierten Feldstudie zum vorgestellten SnapMe-Dienst.

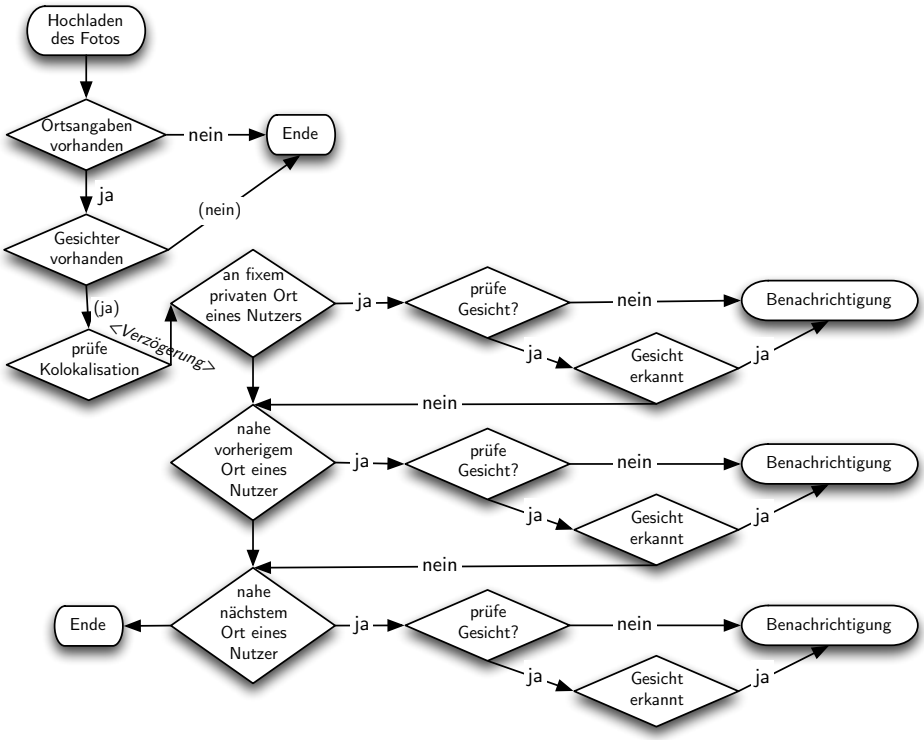


Abbildung 5.32: Kombination von Kollokationsprüfung und Gesichtserkennung für die Prüfung eines Fotos auf Relevanz für die Nutzer durch SnapMe

5.6.1.3 Inferenz

Die Verzögerung der Prüfung und das Vorhalten der Informationen zu Nutzern und Bildern ermöglicht es, auf Basis dieser Informationen weitere Prüfungen durchzuführen. So lässt sich beispielsweise durch Inferenz feststellen, ob eine Person auf einem Bild abgelichtet sein könnte, wenn zwei Fotos quasi zeitgleich am selben Ort aufgenommen wurden und die Person auf dem anderen der zwei Bilder gefunden wurde. Oder eine zweite Person wurde auf einem Bild erkannt, welche kurz davor mit der betrachteten Person zusammen auf einem anderen Bild erkannt wurde. In diesem Fall liegt die Vermutung nahe, dass das spätere Bild auch für die betrachtete Person relevant sein könnte. Zu möglichen Methoden der Identifizierung von Personen auf Basis von Kontextinformationen und Inferenz gibt Varshney [145] einen Überblick.

5.6.2 Privatsphäre-Bewertung

Der SnapMe-Dienst kann Nutzern helfen, einen besseren Überblick über die Fotos zu haben, welche ihre Privatsphäre beeinflussen könnten. Wie bei den in Abschnitt 5.5 präsentierten Konzepten muss auch für diesen Dienst bedacht werden, dass dieser selbst Bedrohungen für die Privatsphäre verursachen kann.

Durch die Festlegung fixer privater Orte geben die Nutzer dem SnapMe-Dienst gegenüber preis, welche Orte für sie privat sind, wo sie wohnen oder arbeiten. Die daraus resultierende Bedrohung kann abgemildert werden, indem die Koordinaten nicht exakt gewählt werden und der Radius des Kreises entsprechend vergrößert wird. Auch zeitliche Einschränkungen können grober gewählt werden, um SnapMe gegenüber nicht zu viel preiszugeben. Nutzer könnten außerdem zusätzlich falsche fixe private Orte definieren. Die Möglichkeit, die eigene Privatsphäre auf diese Weise zu schützen, muss jedoch vom Anbieter im Sinne der Anzahl und der Radiusgröße der fixen privaten Orte eingeschränkt werden: Einerseits um bei einer alleinigen Prüfung auf Kollokation nicht unnötig viele falsch-positive Benachrichtigungen entstehen zu lassen. Andererseits um die Anzahl notwendiger Prüfungen wie die Gesichtserkennung infolge der Kollokationsprüfung im möglichen Rahmen zu halten.

Die Verwendung des standortbezogenen Dienstes für den dynamischen privaten Ort eines Nutzers ist eine weitere Quelle möglicher Bedrohungen der Privatsphäre. Die Nutzer teilen ihren aktuellen Aufenthaltsort mit dem SnapMe-Dienst. Ihr Aufenthaltsort kann direkt mit ihrem Nutzerkonto in Verbindung gebracht werden. Der Dienst nutzt die Ortsinformationen für die Prüfung der geographischen Kollokation und kann sie später verwerfen. Die Informationen müssen für eine gewisse Zeitspanne vorgehalten werden, aber nicht auf Dauer gespeichert werden. Wollen sie die Funktion des dynamischen privaten Ortes verwenden, müssen die Nutzer darauf vertrauen, dass der Anbieter die Informationen nicht missbraucht.

Für die Prüfung der dynamischen privaten Orte müssen auch Ortsinformationen zu Bildern für eine gewisse Zeit vorgehalten werden. Die Nutzer müssen darauf vertrauen, dass die Ortsangaben zu Bildern und zu Nutzern durch den Anbieter ausreichend geschützt werden und dass diese später gelöscht werden.

Die Ortsinformationen zu einem dynamischen privaten Ort dürfen nicht verschleiert werden, da dies dazu führen würde, dass die Prüfung auf falschen Daten beruht und somit wahrscheinlich keine korrekterweise relevanten Fotos gefunden würden. Wie bei den vorherigen Konzepten zur Unterstützung der aktiven Suche könnte auch hier ein gewisser Schutz der Privatsphäre dadurch realisiert werden, dass neben realen Ortsangaben auch gefälschte Orte an den SnapMe-Dienst übergeben werden. Da jedoch alle diese in eine Relevanzprüfung einfließen und die Nutzer nicht die eine korrekte aus mehreren Antworten wählen können, müsste die SnapMe-Implementierung diese Art von Schutz aktiv unterstützen, so dass ein Nutzer mehrere dynamische pri-

vate Orte parallel besitzen könnte und die Ortsangaben zu diesen nicht verschwimmen. Diese Art von Schutz erschwert dem Dienstanbieter jedoch wieder nur den wahren Ort des Nutzers zu erfahren, wie schon zuvor beschrieben wurde. Da durch diese Art des Schutzes die Last für das Gesamtsystem merklich steigt, ist fraglich, ob ein Anbieter die notwendige Unterstützung implementieren würde.

Aktiviert ein Nutzer den SnapMe-Client zur Aktualisierung seines dynamischen privaten Ortes nur in bestimmten Situationen, so kann der Anbieter daraus Informationen über den Nutzer ableiten, da dieser auf diese Weise die für ihn wirklich privaten Orte verrät. Um diesem und dem vorherigen Problem zu begegnen, wäre eine kombinierte Lösung eine mögliche Option: In wirklich privaten Situationen sendet der Client die reale Position des Nutzers und in der übrigen Zeit werden verfälschte Ortsinformationen übermittelt. SnapMe würde in diesem Fall Unregelmäßigkeiten in den Daten feststellen, es wäre jedoch schwerer zu erraten, bei welchen es sich um Angaben des realen Ortes handelt.

Nutzer des SnapMe-Dienstes können Bedenken haben, dass die Funktion zum Schutz der Privatsphäre gleichzeitig dafür sorgen kann, dass auch unerwünschte Bilder schneller verbreitet werden. Diesen Bedenken muss recht gegeben werden. Wie im Fall der zu akzeptierenden Privatsphäre-Kompromisse müssen sich die Nutzer auch mit dieser Einschränkung arrangieren, wenn sie von der Funktion profitieren wollen. Es kann passieren, dass sich auch manch unerwünschtes Foto schneller verbreitet, jedoch würden ohne den SnapMe-Dienst auch viele Fotos von den betroffenen unentdeckt bleiben und sie könnten gegen diese nichts unternehmen.

Ein Aspekt, der ebenso beachtet werden muss, ist die Sicherstellung dessen, dass fixe private Orte nicht für die Überwachung von Orten ausgenutzt werden können, indem diese allein auf Basis von geographischer Kollokation überwacht werden. Eine Möglichkeit wäre für diese privaten Orte zusätzliche Prüfungen durch SnapMe zu erzwingen. Nutzer könnten alternativ die Legitimität ihres Interesses an einem Ort anderweitig nachweisen, indem sie beispielsweise ihr regelmäßiges Aufhalten an diesem Ort über den Standortdienst von SnapMe nachweisen.

5.6.3 Zugriff auf relevante Bilder

Das Ziel des hier präsentierten Ansatzes ist in erster Linie die Identifizierung relevanter Bilder, über die ein Nutzer informiert werden sollte, um seine Privatsphäre eigenhändig schützen zu können. Nicht im Detail behandelt wird daher der im Weiteren wichtige Aspekt der Zugriffskontrolle für die relevanten Bilder. SnapMe kann auch Bilder als relevant identifizieren, auf welche eine betroffene Person keinen Zugriff hat. Wird der Ansatz umgesetzt, so ist die Ermöglichung von Zugriff ein weiteres, sehr interessante Forschungsthema.

Im einfachsten Fall würde der Nutzer nur über die Fotos informiert werden, für die er regulär die notwendigen Zugriffsberechtigungen besitzt. Eine Alternative wäre, dass alle Nutzer der SnapMe-Erweiterung in beiderseitigem Einvernehmen den Personen, welche sich nahe einer Aufnahme befunden haben, den Zugriff zum jeweiligen Bild erlauben. Der Nachweis könnte auf Basis der Informationen der dynamischen privaten Orte geschehen. Hierbei muss aber sichergestellt sein, dass die Informationen nicht gefälscht werden können, damit sich niemand einen nicht legitimen Zugang zu Bildern erschleichen kann. Alternativ könnten andere Methoden des Nachweises von Nähe verwendet werden, die auf der Interaktion der Geräte von Fotograf und Fotografiertem beruhen. Ein möglicher Ansatz wären eventuell Techniken basierend auf Bluetooth Low Energy, wie Apples iBeacon-Standard. Wichtig ist, dass durch die Nachweise keine weiteren Bedrohungen für die Privatsphäre entstehen.

Eine andere Möglichkeit wäre den Fotografierten und den Fotografen über einen standardisierten Weg miteinander kommunizieren zu lassen, so dass sie den Zugriff auf ein betroffenes Bild aushandeln könnten, ähnlich der Nutzer-Kooperation die Besmer et al. [78] für *Restrict Others* nutzten.

5.6.4 Machbarkeitsnachweis mittels Simulation

Um einen grundlegenden Einblick in die Effektivität des SnapMe-Dienstes und den Einfluss der verschiedenen Parameter zu erlangen, wurde das Konzept mit dem in Anhang A präsentieren *Mobile Security & Privacy Simulator* evaluiert [108, 106].

Architektur In Abbildung 5.33 wird das Zusammenspiel der beteiligten Komponenten skizziert. Der SnapMe-Dienst wurde in vereinfachter Form auf Basis von PHP, MySQL und dem Apache-Webserver implementiert: Die Registrierung der Nutzer, ein Mechanismus zum Hochladen fiktiver Fotos mit Ortsangaben sowie ein Mechanismus zur Verarbeitung der aktuellen Standorte der Nutzer wurden auf dem Webserver implementiert. Hochgeladene Fotos und erhaltene Aufenthaltsorte wurden in der Datenbank gespeichert und im Folgenden von Hintergrundprozessen verarbeitet. Die Hintergrundprozesse führten die Prüfung auf Kollokation und die statistikbasiert simulierte Gesichtserkennung durch und speicherten die Ergebnisse für die spätere Auswertung. Die Nutzer, ihre Bewegung, das Fotografieren und anschließende Hochladen zum Webserver sowie die Standortaktualisierungen für die dynamischen privaten Orte wurden simuliert. Um ein korrektes Timing der realen und simulierten Teile sowie eine korrekte Einhaltung definierter Verzögerungsintervalle zu gewährleisten, verwendeten alle Komponenten eine fiktive Zeit, deren Fortschreiten durch die Simulation gesteuert wurde.

Simulationsszenario In der durchgeführten Simulation bewegten sich die Personen innerhalb von Downtown Chicago. Zu Beginn der Simulation wurden die

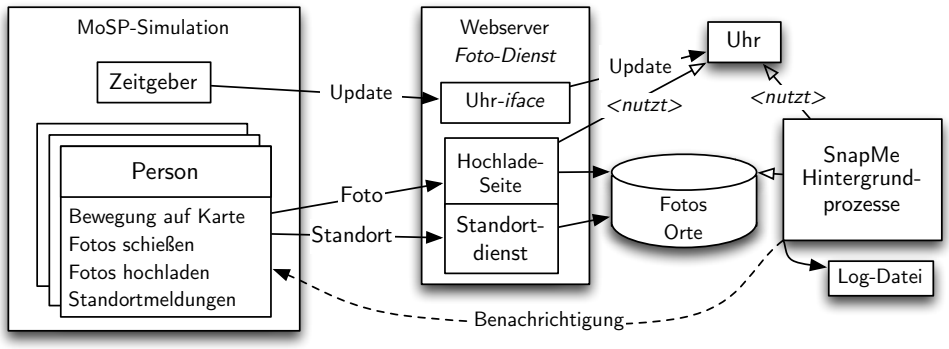


Abbildung 5.33: Architektur der Evaluation des SnapMe-Konzepts mittels Simulation

Nutzer zufällig auf der Straßenkarte platziert. Die Bewegung einer Person verlief zufällig von einem Wegpunkt zum nächsten, an welchem sie jeweils für eine zufällige Zeit von bis zu 30 Sekunden stoppte. Kam eine Person an einem der 122 in den OpenStreetMap-Kartendaten spezifizierten Cafés oder einem der 46 manuell hinzugefügten öffentlichen Plätze vorbei, so stoppte sie dort mit einer 50-prozentigen Wahrscheinlichkeit für eine zufällige Zeit zwischen einer halben Minute und 30 Minuten. Abbildung 5.34 zeigt die verwendete Karte mit den beschriebenen Verweilorten. Der genaue Verweilort im Café oder beispielsweise auf einer Grünfläche wurde durch Zufall innerhalb eines Kreises mit einem in den Kartendaten festgelegten ortsspezifischen Radius gewählt, um die Personen an diesen Orten in der Fläche zu platzieren.

Jeder Durchlauf simulierte eine Zeitspanne von 8 Stunden. Es wurden ausschließlich aktive (fotografierende) und passive (nur benachrichtigte) SnapMe-Nutzer simuliert. Andere Personen wurden nicht berücksichtigt, da diese weder in Betracht gezogene Fotos hochgeladen hätten, noch über Fotos informiert worden wären. Der Anteil an aktiven Nutzern an der Gesamtnutzerzahl mit einem Wert von 35 % wurde Statistiken zum Dienst Instagram [45] entnommen.

Ebenfalls basierend auf den Statistiken zu Instagram sowie Statistiken zu Facebook [32] schossen und teilten die simulierten Fotografen alle 43 Stunden ein Foto. Die Nutzungsstatistiken zu Instagram, einem der rasant wachsenden Dienste zum Teilen von Fotos, zeigten, dass im März 2011 die durchschnittliche Zeit zwischen dem Hochladen zweier Bilder eines Nutzers 43 Stunden betrug. Im September 2012 hatte Facebook eine Milliarde Nutzer von denen täglich circa die Hälfte den Dienst nutzten. Durchschnittlich wurden zu diesem Zeitpunkt mehr als 300 Millionen Fotos pro Tag hochgeladen. Dies entspricht einem durchschnittlichen Werte zwischen 0,6 und 0,3 Fotos pro Nutzer pro Tag, woraus sich eine durchschnittliche Zeit zwischen zwei Fotos eines Nutzers zwischen 40 und 80 Stunden ergibt. Unter der Annahme, dass vorwiegend die aktiven Nutzer Fotos hochladen, bestätigen die Zahlen zu Facebook somit die Zahlen zu Instagram, welche für die Simulation verwendet wurden. Der Zeitpunkt des nächsten Fotos wurde daher für jeden Fotografierenden zufällig

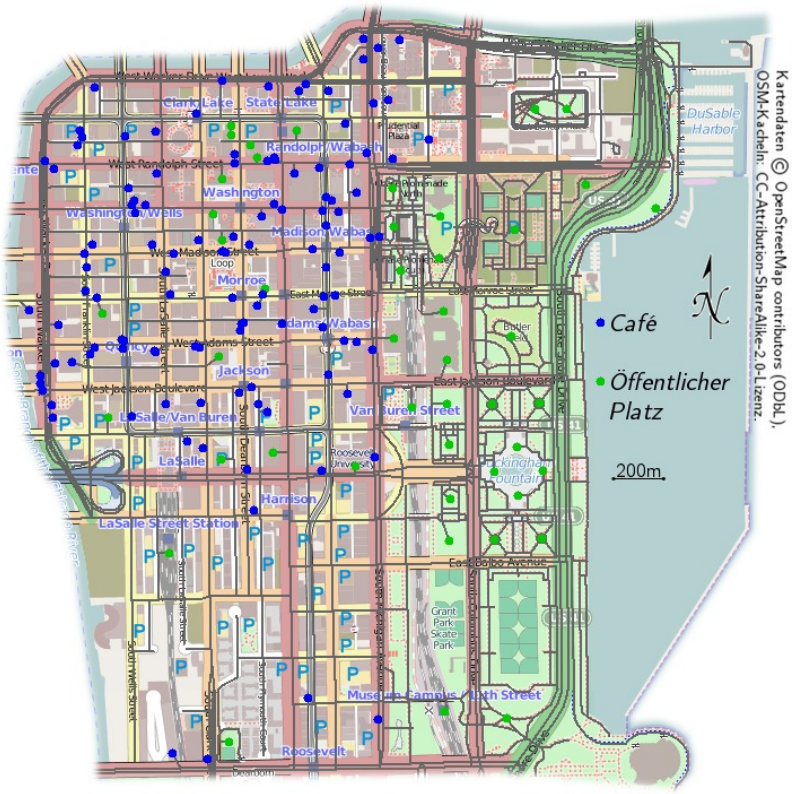


Abbildung 5.34: Karte der SnapMe-Simulation mit Verweilorten

innerhalb der nächsten 43 Stunden ab Simulationsstart festgesetzt. Somit haben in einem Simulationslauf im Mittel $^{8}/_{43}$ der aktiven Nutzer ein Foto gemacht.

In Anlehnung an die technischen Spezifikationen von typischen Kamera-Handys wurde ein Bildwinkel von 62° gewählt. Als „Reichweite“ eines Fotos wurden 10 Meter angenommen, so dass Personen innerhalb des Gegenstandsraumes bis zu dieser Distanz von einem fiktiven Bild erfasst wurden. Die Richtung jedes Fotos wurde zufällig gewählt. Ein fiktives Foto bestand aus Informationen über die Personen, welche sich im abgebildeten Bereich befanden, sowie aus der Zeit und dem Ort des Fotos. Zu jeder abgebildeten Person wurde der eindeutige Identifikator erfasst sowie ein Zufallswert, der die Erkennbarkeit des Gesichtes bestimmte. Nachdem ein Foto geschossen wurde, wurde es ohne Verzögerung beim Fotodienst mit SnapMe-Erweiterung hochgeladen.

Beim Hochladen wurde das Foto vom Webdienst entgegengenommen und in der Datenbank gespeichert. Mit einer Verzögerung von 45 Minuten wurde ein Foto geprüft, so dass Standortaktualisierungen anderer Nutzer nach dem Zeitpunkt des Fotos ausreichend berücksichtigt wurden. Für die Prüfung eines Fotos wurde der in Abbildung 5.32 gezeigte Ablauf umgesetzt, wobei Fotos ohne Gesichter verworfen wurden. Für eine exakte Berechnung von Distanzen zur Prüfung auf Kollokation wurden die geographischen Koordinaten in UTM-Koordinaten transformiert.

Die Erkennung und Wiedererkennung von Personen auf den Fotos wurde durch statistische Entscheidungen auf Basis wissenschaftlich publizierter Erfolgsraten realisiert. Ein einzelnes Ergebnis wurde durch die Erkennbarkeit der Gesichter bestimmt, die zuvor durch die Simulation bestimmt worden war.

Für die Prüfung, ob Personen auf einem Bild abgebildet sind, wurde die Gesichtserkennung als empfindlich eingestellt angenommen, um möglichst keine Bilder mit Personen auszuschließen. Eine hohe Empfindlichkeit der Erkennung sorgt für eine ebenso höhere Zahl fälschlicherweise erkannter Gesichter, jedoch erzeugt die Erkennung von Bildern ohne Gesichter als Bilder mit Gesichtern lediglich mehr Last in der anschließenden Prüfung und hat keine Auswirkungen auf den Privatsphäreschutz. Basierend auf [94] wurde eine Hit-Rate von 95 % und eine False-Alarm-Rate von 1 % angenommen. Für die Wiedererkennung von Gesichtern wurde basierend auf [129] eine durchschnittliche False-Reject-Rate von 30 % in Kombination mit einer False-Accept-Rate von 1 % gewählt. SnapMe nutzt Gesichtserkennung, um die Relevanzprüfung für einzelne Nutzer zu verbessern und so die Zahl der Benachrichtigungen zu verringern. Die False-Accept-Rate wirkt sich auf die Zahl der Benachrichtigungen und die Zahl der zu prüfenden Fotos aus, was aus Sicht der Privatsphäre am ehesten toleriert werden kann. Eine hohe False-Reject-Rate erhöht hingegen die Zahl fehlender Benachrichtigungen. Daher sollte diese so gering wie möglich sein.

Die Aktualisierungen des eigenen Standortes für die dynamischen privaten Orte machten alle Nutzer mit demselben Zeitintervall beginnend an einem individuellen, zufallsbestimmten Startzeitpunkt. Ebenso wie das Aktualisierungsintervall wurden die Radien der privaten Orte je Simulationslauf für alle Personen identisch festgelegt. Bei der Evaluierung der fixen privaten Orte wurde die Startposition eines Nutzers als sein fixer privater Ort konfiguriert.

Ergebnisse

Mit der Simulation wurden die fixen privaten Orte und die dynamischen privaten Orte separat mit verschiedenen Parameterwerten evaluiert. Im Folgenden werden die Ergebnisse für 500 bis 10.000 simulierte SnapMe-Nutzer ausschnittsweise präsentiert.

Die besten Ergebnisse wurden bei der Verwendung der dynamischen privaten Orte in Kombination mit der Gesichtserkennung erzielt. Tabelle 5.8 zeigt für diese Variante die Effektivität der Benachrichtigung (Anteil der benachrichtigten abgelichteten Personen) für verschiedene Radien und Aktualisierungsintervalle. Je kürzer das Aktualisierungsintervall war, desto höher war die Effektivität des Dienstes. Die schlechteren Werte für kleinere Radien lassen sich damit erklären, dass nur die gemeldeten aktuellen Orte verglichen wurden und keine Interpolation für Aufenthaltsorte zwischen diesen durchgeführt wurde. Bei den längeren Aktualisierungsintervallen steigt die Effektivität langsamer mit dem Radius. Bei den dynamischen privaten Orten mit zusätzlicher Gesichtserkennung scheint die Effektivität eingeschränkt un-

abhängig von der Nutzerzahl zu sein, wie Tabelle 5.9 zeigt. Je mehr Personen auf einem Foto sind, desto mehr werden auch erkannt und informiert. Gleichzeitig werden durch mehr Fotografen auch mehr Fotos gemacht, die durch das Raster der Prüfung fallen können. Die Effektivität des Konzepts hängt vorwiegend vom gewählten Radius und dem Aktualisierungsintervall ab. Mit einer Aktualisierung im 15-Minutentakt und einem Privatsphäre-Radius von 20 Metern wurden die Nutzer über fast die Hälfte aller Abbildungen auf Fotos informiert.

Benachrichtigungen abgelichteter Personen
∅ 380 Fotos mit 164 Fotografierten

	Aktualisierungsintervall		
Radius	5 Min.	10 Min.	15 Min.
10 m	45 %	53 %	46 %
20 m	57 %	62 %	49 %
50 m	78 %	60 %	54 %
100 m	77 %	69 %	57 %

Tabelle 5.8: Effektivität der dynamischen privaten Orte plus Gesichtserkennung bei 5.000 simulierten SnapMe-Nutzern

Benachrichtigungen abgelichteter Personen
(absolute Zahl abgelichteter Personen)
Aktualisierungsintervall: 5 Minuten

	Anzahl SnapMe-Nutzer			
Radius	500	1.000	2.000	10.000
10 m	67 % (3)	100 % (2)	74 % (34)	27 % (677)
20 m	100 % (2)	50 % (2)	78 % (27)	51 % (541)
50 m	0 % (1)	80 % (5)	66 % (29)	67 % (557)

Tabelle 5.9: Effektivität der dynamischen privaten Orte plus Gesichtserkennung bei variierender SnapMe-Nutzerzahl

Wie Tabelle 5.10 erkennen lässt, hat die reine Verwendung der fixen privaten Orte eine geringe Effektivität. In diesen Fällen werden die Personen nur über Fotos informiert, wenn sie im Umkreis ihres fixen privaten Ortes fotografiert werden, was seltener passierte, als wenn ihnen ihr privater Bereich wie ein Schatten folgte. Dies zeigt, dass statische Verfahren, wie Flickrs Geofence wohl nur verwendet werden sollten, um Foto an speziellen Orten vor anderen im Sinne von Zugriffsschutz zu verbergen. Sowohl die fixen als auch die dynamischen privaten Orte sind ohne die zusätzliche Verwendung von Gesichtserkennung wohl nur in Bereichen mit wenig Dienstnutzern verwendbar, da sonst die Zahl der gemeldeten Fotos explodiert, so dass die Zahl der zu kontrollierenden Fotos schnell über das manuell kontrollierbare Maß hinaus wächst, selbst wenn die Zahl der Benachrichtigungen beispielsweise durch periodische Zusammenfassungen im Zaum gehalten werden könnte. Die Gesichtserkennung verringert die Zahl der falsch-positiven Benachrichtigungen auf eine handhabbare Größe.

5.000 Personen, Aktualisierungsintervall: 5 Minuten	*Radius*	*# Fotos*	*# Fotos mit Personen*	*# abgebildeter Personen*	*# Benachrichtigungen*	*# Benachrichtigungen pro abgeb. Person*
1. fixe private	50	390	65	165	6	0,04
Orte mit	100	383	55	215	15	0,07
Gesichtserkennung	250	381	70	192	37	0,19
2. fixe private	50	379	51	139	8.940	64,3
Orte ohne	100	385	50	146	18.190	124,6
Gesichtserkennung	250	380	60	160	57.472	359,2
3. dynamische private	10	386	63	136	1.767	13
Orte mit	20	392	60	181	4.346	24
Gesichtserkennung	50	391	61	156	15.965	102,3

= Anzahl

Tabelle 5.10: Vergleich verschiedener Prüfungen für 5.000 SnapMe-Nutzer

5.6.5 Proof-of-Concept-Implementierung

Um die Umsetzbarkeit des Dienstes weiter zu evaluieren, wurden die Grundfunktionen als Proof-of-Concept implementiert. Die Implementierung und einige durch diese identifizierten Herausforderungen werden im Folgenden beschrieben.

5.6.5.1 SnapMe-Dienst

Der SnapMe-Dienst wurde auf Basis der Skriptsprache *Python* und dem Framework *CherryPy* implementiert. Für die Speicherung von Informationen zu Bildern und privaten Orten wurde die *PostgreSQL*-Datenbank verwendet. Durch die Verwendung der *PostGIS*-Erweiterung konnten geographische Objekte direkt in der Datenbank gespeichert werden und räumliche Anfragen gestellt werden. Für die Gesichtserkennung wurde *OpenCV* verwendet.

Webseite Die Webseite des Proof-of-Concepts dient primär der Konfiguration des SnapMe-Dienst-Profils eines Nutzers. Wie in Abbildung 5.35 dargestellt, kann ein Nutzer dort seine fixen privaten Orte durch das Positionieren von Kreisen auf einer Karte festlegen, sie verändern oder löschen. Die grafische Nutzerschnittstelle erleichtert das Verständnis der privaten Orte und zeigt dem Nutzer ihre Ausdehnung, so dass ihm bewusst ist, wie weit ein definierter Radius reicht und seine Privatsphäre schützt. Eine entsprechende Visualisierung für den dynamischen privaten Ort eines Nutzers könnte in der Client-App realisiert werden. Über die Webseite können Bilder für das Training der Gesichtserkennung hochgeladen werden, wenn diese beispielsweise nicht von einem verbundenen Fotodienst bezogen werden. Der Nutzer kann festlegen, ob er nur auf Basis von Kollokation informiert werden will oder ob

die Gesichtserkennung verwendet werden soll. Des Weiteren kann der Nutzer eine Standard-Zeitzone festlegen, die beim Fehlen dieser Information verwendet wird, sein Passwort ändern oder die E-Mail-Adresse für Benachrichtigungen festlegen.

Abbildung 5.35: SnapMe-Webseite zur Definition fixer privater Orte

SnapMe als Facebook-App Die Proof-of-Concept-Implementierung ermöglicht einem Nutzer, seinen SnapMe-Account über die Webseite mit einem Facebook-Account zu verbinden. Durch die Facebook-Integration von SnapMe als Facebook-App können Bilder, die beim SnapMe-Dienst hochgeladen und dort geprüft werden, von SnapMe im Namen des Nutzers automatisch bei Facebook geteilt werden. Über die SnapMe-Konfiguration kann festgelegt werden, mit welchen Zugriffsbeschränkungen ein Bild standardmäßig geteilt wird. Während das SnapMe-Konzept eine tiefe Integration in einen Fotodienst vorsieht, wurde diese Lösung für die Evaluierung gewählt. Nutzer können so ihre Fotos wie gewohnt bei Facebook teilen, jedoch auch die Bewusstsein schaffende Funktion nutzen. Für eine zukünftige Feldstudie innerhalb einer geschlossenen Nutzergruppe wäre dies ausreichend, für einen wirklichen Betrieb jedoch nicht, da nur von SnapMe-Nutzern geteilte Fotos geprüft werden, während das SnapMe-Konzept davon ausgeht, alle geteilten Fotos zu prüfen.

Bild hochladen Um ein Bild über die Client-App hochzuladen, wurde eine Web-API implementiert. Als optionale Parameter können beim Hochladen jeweils der Ort und die Zeit des Bildes und des Clients sowie die Zeitzone des Clients angegeben werden. Außerdem kann der Client bestimmen, ob der Ort als dienstinterne Metainformation übernommen werden soll.

Um das Bild im Weiteren prüfen zu können, werden der Ort und die Zeit der Aufnahme über eine Heuristik bestmöglich bestimmt. Wurden Koordinaten für den Ort des Bildes als Parameter übergeben, so werden diese verwendet. Dies ermöglicht, die Extraktion von Metadaten auf den Client auszulagern. Andernfalls werden eventuell vorhandene Koordinaten aus den integrierten Bild-Metadaten durch den SnapMe-Dienst extrahiert. Kann auf diese Weise kein Ort festgestellt werden, werden die Koordinaten des Clients verwendet. Kann kein Ort festgestellt werden, wir das Bild nicht durch SnapMe geprüft. Für die Bestimmung des Aufnahmezeitpunktes wird identisch vorgegangen. Dabei wird auf alle Zeitangaben außer dem GPS-Zeitstempel, welcher per Definition in Form der koordinierten Weltzeit vorliegt, die Zeitzone des Clients angewendet. Da die gängigen integrierten Bild-Metadaten die Angabe einer Zeitzone nicht unterstützen und SnapMe auf das spontane Teilen von Fotos ausgelegt ist, ist dies die beste Lösung, da vermutet werden kann, dass geteilte Fotos meist auch mit dem Client oder zumindest in derselben Zeitzone erstellt worden sind. Um weitere Probleme durch Zeitzonen zu vermeiden, wird die gewählte Zeit in Form der koordinierten Weltzeit gespeichert. Liegen mehrere Zeiten als integrierte Metadaten vor, so wird der GPS-Zeitstempel aus dem zuvor genannten Grund bevorzugt.

Nach der Bestimmung von Ort und Zeit wird das Bild in die Bildersammlung des Nutzers aufgenommen, gegebenenfalls bei Facebook geteilt und für die Prüfung vorgemerkt. Wird bei der Zeitermittlung festgestellt, dass das Bild zu jenem Zeitpunkt älter als eine Stunde war, wird es nicht geprüft, da keine vergleichsfähigen dynamischen Standortinformationen mehr vorliegen und zudem die zugrunde gelegte Spontanität des Teilens nicht mehr gegeben ist. Ebenfalls wird das Bild nicht geprüft, wenn es deutlich in der Zukunft liegt, da ein Vergleich nicht sinnvoll ist, wenn ein Nutzer die notwendige Zeit der Aufnahme ersichtlich falsch eingestellt hat.

Dynamische Standortinformationen Über die Web-API des SnapMe-Dienstes können Nutzer ihren aktuellen Ort mitteilen, der zusammen mit der aktuellen Uhrzeit gespeichert wird. An dieser Stelle ist es ratsam die Häufigkeit der Aktualisierungen serverseitig zu beschränken, um den Ortsdatenbestand nicht zu sehr wachsen zu lassen und die Datenbankanfragen bei der Prüfung nicht unnötig zu verlangsamen. Heutige mobile Geräte geben eine Genauigkeit des festgestellten Standortes an. Diese wird ebenfalls von SnapMe erfasst und kann so in den real berücksichtigten Radius der dynamischen privaten Orte einkalkuliert werden. Ein Hintergrundprozess entfernt Daten aus dem Ortsdatenbestand, sobald sie so weit gealtert sind, dass sie für keine Prüfungen mehr verwendet werden.

Prüfung Sobald die festgelegte Verzögerungszeit für ein neues, zu prüfendes Foto verstrichen ist, kann die Prüfung auf Relevanz von einem Hintergrundprozess durchgeführt werden. Sie wurde wie folgt implementiert:

Zuerst wird das Bild wie zuvor beschrieben auf enthaltene Gesichter geprüft. Für die Detektion von Gesichtern werden dabei die mit OpenCV bereitgestellten *Haar-Klassifikatoren* verwendet. Bildausschnitte gefundener Gesichter werden für den Vergleich mit SnapMe-Nutzern zwischengespeichert.

Als Nächstes wird das Bild auf Kollokation mit fixen oder dynamischen privaten Orten der registrierten Nutzer geprüft. Momentan wird die Kompassrichtung eines Bildes nicht berücksichtigt. Ein Bild wird somit wie die privaten Bereiche als Kreis (sonst: Kreissegment) mit den jeweiligen Koordinaten als Mittelpunkt modelliert. Als „Reichweite“ eines Bildes (Kreisradius) wird eine feste Distanz verwendet. Die Reichweite könnte in einer späteren Umsetzung auf Basis der Informationen zu Kamera und Objektiv in den integrierten Bild-Metadaten individuell angepasst geschätzt werden. Die privaten Orte liegen in der Datenbank direkt als räumliche Objekte vor. Durch spezielle PostGIS/PostgreSQL-Anfragen mit einer Filterung nach Abstand zwischen den geometrischen/geographischen Objekten des Fotos und der privaten Orte können kollokalisierte private Orte direkt festgestellt werden. Wird keine Kollokation festgestellt, wird die Prüfung beendet. Andernfalls wird für jeden Nutzer, für den eine Kollokation festgestellt wurde, die Prüfung fortgeführt.

Hat ein Nutzer die Verwendung von Gesichtserkennung deaktiviert, so wird er direkt benachrichtigt. Für die übrigen Nutzer wird jedes anfänglich detektierte Gesicht mit den Modellen ihrer Gesichter verglichen, welche aus den von ihnen bereitgestellten Trainingsbildern erstellt wurden. Für die Wiedererkennung von Nutzern wird das Gesichtserkennungsmodell *Local Binary Patterns Histograms* (LBPH) verwendet. Ein Vorteil dieses Modells gegenüber anderen wie *Fisherfaces* oder *Eigenfaces* ist, dass bei LBPH das Modell eines Gesichtes im Verlauf der Benutzung durch das Trainieren mit weiteren Bildern verbessert werden kann und nicht komplett neu trainiert werden muss. Somit müssen Vergleichsbilder der Nutzer nicht dauerhaft gespeichert werden, was aus Sicht des Privatsphäreschutzes zu begrüßen ist. Wird eine kollokalisierte Person ausreichend gut auf dem Foto erkannt, wird sie über das Bild informiert und die Prüfung beendet. Wird eine der Personen nicht erkannt, wird sie hingegen nicht benachrichtigt.

Benachrichtigung Ein Nutzer wird durch eine E-Mail informiert, dass ein relevantes Foto gefunden wurde.

5.6.5.2 Client-App

Die für das mobile Betriebssystem Android entwickelte App ermöglicht, den aktuellen Standort eines Nutzer für die Nutzung des dynamischen privaten Ortes an den SnapMe-Dienst zu übermitteln. Über die Client-App kann ein Nutzer seinen aktuellen Standort einmalig an SnapMe senden oder ihn über einen Hintergrunddienst in einem regelmäßigen Intervall zwischen einer und 60 Minuten an den Dienst senden lassen. Auch den Privatsphäre-Radius des dynamischen privaten Ortes, welcher zwischen 10 und 50 Metern liegen darf, legt der Nutzer in der App fest.

Die App erlaubt dem Nutzer zudem, ein Foto zum SnapMe-Dienst hochzuladen. Dazu kann er über die App ein Foto aus der Bildergalerie auswählen oder er kann ein Bild aus einer anderen App über die *Teilen-über*-Funktion von Android an die App übertragen, die dieses daraufhin hochlädt. Neben dem Foto werden dabei die zuvor beschriebenen Parameter ebenfalls an den Server übertragen.

Abbildung 5.36 zeigt den Hauptbildschirm der Android-App sowie die Teilen-über-Funktion beim Teilen eines Bildes in der App *Galerie*.

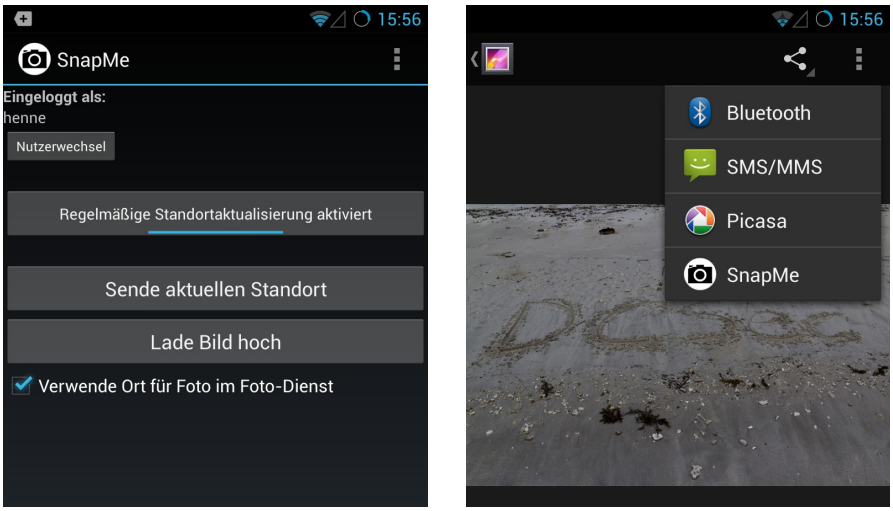


Abbildung 5.36: SnapMe-Android-App: Hauptmenü und *Teilen-über*-Funktion

5.7 Zusammenfassung

Dieses Kapitel hat sich mit der fremdverursachten Bedrohung durch geteilte Fotos und Metadaten beschäftigt, derer sich die Nutzer nicht bewusst sind.

Eine Analyse einer Auswahl von Webdiensten, die zum Teilen von Fotos verwendet werden, hat gezeigt, wie unterschiedlich die Dienste sowohl Zugriffsschutzmechanismen als auch die Verarbeitung von Bild-Metadaten umsetzen. Besonders der vielfältige Umgang mit Metadaten und insbesondere eingebetteten Metadaten macht es für die Nutzer schwierig einen Überblick zu haben, welche Informationen mit Fo-

tos durch sie und vor allem durch andere im Web geteilt werden. Metadaten können die Bedrohung durch Fotos verstärken oder sogar erst entstehen lassen, indem sie Kontextinformationen zu abgelichteten Situationen bereitstellen.

Eine Analyse privatsphärerelevanter Metadaten von über 200.000 Fotos der Fotodienste Flickr und Locr hat gezeigt, wie häufig verschiedene Arten von Metadaten momentan von den Nutzern mit Bildern im Web geteilt werden. Während Fotos klassischer Digitalkameras vermehrt solche Metainformationen enthalten haben, die vorwiegend manuell zu Bildern hinzugefügt werden, haben die Fotos von mobilen Geräten vor allem solche Metadaten enthalten, die automatisiert und damit oft unbewusst in die Bilder integriert werden. Da der Anteil der als Kamera verwendeten mobilen Geräte wie Smartphones oder Tablets weiterhin steigt und außerdem auch zunehmend Metainformationen – allen voran privatsphärerelevante koordinatenbasierte Ortsangaben und zukünftig vermutlich Personen-Markierungen – automatisiert in den Bildern gespeichert werden ist mit einer steigenden Bedrohung durch Metadaten und die dazugehörigen Bilder zu rechnen.

Um das aktuelle Bewusstsein der Nutzer zu beurteilen, wurde eine Online-Umfrage durchgeführt. Die Ergebnisse der Umfrage zeigen deutlich, dass sich die 414 Teilnehmer nicht ausreichend über im Web geteilte, sie betreffende Fotos informiert fühlen. Sie wünschten sich Unterstützung, um sich besser informieren zu können. Die Teilnehmer zeigten im Rahmen der Umfrage eine deutliche Meinung zur Privatheit verschiedener Metainformationen, wie beispielsweise dem Aufnahmeort eines Bildes. Trotzdem war ein nennenswerter Teil der Teilnehmer bereit, sich zumindest theoretisch konzeptionell auf die Idee der Privatsphäre-Kompromisse einzulassen: Sie würden einige weniger als privat erachtete Informationen preisgeben, um als mehr privat erachtete Informationen zu schützen.

Um das Bewusstsein der Nutzer über geteilte Fotos und Metadaten nicht nur auf Basis von Selbstauskünften zu beurteilen, wurde im Weiteren eine Studie im Rahmen von Facebook durchgeführt. Durch die Kombination zweier Fragebögen und einer dafür entwickelten App wurde das Ausmaß geteilter Fotos der direkten Freunde von 2.753 Facebook-Nutzern erfasst. Für 2.561 dieser Nutzer wurde das Bewusstsein über das Ausmaß dieser Fotos erfasst. Durch einen Vergleich von Schätzungen und realen Werten konnte beurteilt werden, wie groß das Unvermögen vieler Nutzer ist, die Menge von Bildern und Metadaten annähernd einschätzen zu können. Dies ist ein deutliches Zeichen für unzureichendes Wissen über das Ausmaß der möglichen Bedrohung durch geteilte Fotos. Dies unterstreicht die Notwendigkeit für Methoden zum Schutz der Privatsphäre durch die Schaffung von Bewusstsein: Die Nutzer sollten beurteilen können, ob und wie sehr sie durch geteilte Fotos betroffen sein könnten. Die durch die App ermittelten Zahlen können der allgemeinen Aufklärung und der Bewusstseinsschaffung des Einzelnen dienen. Sie zeigen einen deutlichen

Bedarf für Methoden, die Nutzer ermächtigen, die Fotos zu finden, welche ihrer Privatsphäre schaden könnten.

Für die technische Unterstützung der Nutzer wurden daraufhin zwei verschiedene Ansätze präsentiert. Zuerst wurden Konzepte vorgestellt, die einen Nutzer bei der aktiven Suche nach Fotos unterstützen könnten, indem durch einen Vergleich von Ortsinformationen von Bildern und den Aufenthaltsorten eines Nutzers die Fotos identifiziert werden, bei deren Entstehen der Nutzer zugegen war. Der Tausch von Ortsinformationen gegen Fotos stellt einen Privatsphäre-Kompromiss dar, wie er in Abschnitt 5.3.5 vorgestellt wurde.

Der zweite präsentierte Ansatz geht einen Schritt weiter. Er baut verstärkt auf die von einem nennenswerten Teil der Nutzer als akzeptabel erachteten Privatsphäre-Kompromisse auf und fordert eine stärkere Integration in den Prozess des Teilens eines Fotodienstes. Im Gegenzug ermöglicht er Nutzern, statt durch aktive Suche, durch Benachrichtigungen von Fotos zu erfahren, wenn diese geteilt werden. Die Entscheidung, ob ein Foto für einen Nutzer relevant sein sollte, fußt dabei auch auf dem zuvor verwendeten Vergleich von Ortsinformationen – der Kollokation, jedoch wird zur Verringerung falscher Ergebnisse zusätzlich Gesichtserkennung eingesetzt. Durch Simulation wurde die Funktion des präsentierten Dienstes grundlegend evaluiert und es wurde gezeigt, dass er auch einen Gewinn für die Privatsphäre darstellen könnte. Dabei ist die Verwendung eines standortbezogenen Dienstes für die Kollokationsprüfung von Fotos und Nutzern in Kombination mit Gesichtserkennung die effektivste Lösung. Der Dienst wurde weiter durch die Erstellung einer Proof-of-Concept-Implementierung der Basisfunktionen evaluiert.

Ein Dienst wie der zuletzt präsentierte kann den Nutzern zu einem gewissen Maß helfen, Wissen über solche Fotos zu erlangen, die andere im Web teilen und die ihre Privatsphäre bedrohen könnten. Ein Aspekt für zukünftige Forschung bleibt, wie vom Identifizieren relevanter Bilder über die Benachrichtigung hinaus die Nutzer auch die Zugriffsrechte und ferner die Kontrolle über solche Bilder erlangen können.

In der Praxis muss noch evaluiert werden, wie sich die Nutzer mit Privatsphäre-Kompromissen arrangieren. Den Studienergebnissen nach scheinen diese eine gute Grundlage für Schutzfunktionen zu bieten, da die Nutzer die Privatheit verschiedener Informationen detaillierter zu differenzieren scheinen. Dies deckt sich mit dem Verhalten der sogenannten Privatsphäre-Pragmatisten, wie sie Westin beschreibt: Viele Menschen entscheiden heute von Fall zu Fall über die Preisgabe von Informationen, indem sie die Privatheit von Informationen und den möglichen Einfluss auf ihre Privatsphäre gegen ihren Gewinn abwägen. Dies deckt sich ebenso mit dem Zeitgeist des Web 2.0, in dessen Sinne die Menschen äußerst teil-freudig sind, solange sie in einem guten Licht dastehen, als das der Schutz der Privatsphäre auch verstanden werden kann.

Wird auf Privatsphäre-Kompromisse gebaut, so müssen diese deutlich und verständlich abgesteckt werden: Was wird an wen wie detailliert, wann und wie häufig und wozu preisgegeben. Auch wenn die Nutzer an einer Stelle des Systems aktiv persönliche Informationen preisgeben, müssen diese Informationen im übrigen Design und in der Implementierung eines solchen Dienstes weiterhin gut geschützt werden.

Kapitel 6

Eingebettete Bild-Metadaten

Die Analyse von geteilten Bildern in Abschnitt 5.2 hat gezeigt, dass heute schon eine beachtliche Menge an Metadaten mit Bildern im Web geteilt wird. Gleichzeitig wurde in der Betrachtung der Webdienste in Abschnitt 5.1 gezeigt, wie verschieden der Umgang mit Metadaten von Dienst zu Dienst ist und wie schwer es daher für einen Nutzer sein kann, ein klares Bild vom Umgang mit Kontextinformationen zu bekommen, um resultierende Bedrohungen annähernd einschätzen zu können. Neben den Unterschieden der Webdienste ist zuletzt auch das fehlende Wissen der Nutzer über die Existenz von Metadaten und den Umgang mit diesen als problematisch zu sehen, welches die in Abschnitt 5.3 dargelegten Umfrageergebnisse gezeigt haben.

Wie in der Bedrohungsanalyse beschrieben wurde, können Metadaten sowohl die Verbindung zwischen einer Person und einem Bild herstellen als auch schädlichen Inhalt enthalten. Sie können existierende Bedrohungen durch Bilder verstärken und ebenso selbst Bedrohungen entstehen lassen. Aus diesem Grund werden Metadaten häufig zum einfachen Schutz der Privatsphäre vollständig gelöscht.

Das Löschen eingebetteter Metadaten vor dem Veröffentlichen von Bildern bewahrt betroffene Personen vor der Preisgabe persönlicher oder bedrohlicher Informationen. Auf diese Weise werden jedoch auch nutzbringende Informationen entfernt: Metadaten können dabei unterstützen, die steigende Zahl von Fotos besser zu überblicken und zu kontrollieren. Auf Fotos spezialisierte Dienstanbieter sind fähig, die Masse an Bildern auch ohne Metadaten im Sinne ihres Angebots zu organisieren. Metadaten ermöglichen diesen vor allem das Angebot zusätzlicher Funktionen. Im Gegensatz dazu sind die Nutzer jedoch oft schon mit der Verwaltung ihrer eigenen Bilder überfordert. Besonders ihnen können die Kontextinformationen helfen, den Überblick zu wahren. Aus diesem Grund sollten Metadaten in Bildern erhalten werden, soweit dies mit der Wahrung der Privatsphäre zu vereinbaren ist. Insbesondere gilt dies auch für geteilte Bilder, da mit dem Einsatz mobiler Geräte mehr und mehr Nutzer das Web als primären Speicherort ihrer Bilder verwenden und sich diese im Zweifelsfall von dort herunterladen anstatt vom mobilen Gerät. Werden Metainfor-

mationen erhalten, muss der Schutz privater Informationen auf anderem Wege als dem Löschen durch den Nutzer oder den Dienstanbieter erfolgen. Da es zum Teil auch wünschenswert ist, die Kontextinformationen mit anderen zu teilen, sollten die Nutzer auch die Möglichkeit haben, bewusst zu bestimmen, wer die Kontextinformationen erhält und wer nicht. Die Kontrolle über die Metadaten muss dabei in der Hand des Nutzers liegen, der entscheidet, wer welche Informationen sehen darf und welche Informationen vor dem Teilen doch entfernt werden oder auf anderem Wege geschützt werden. Auf keinen Fall darf dies erst durch einen Dienstanbieter geschehen, da in diesem Fall nicht klar ist, was zuvor mit den Informationen geschieht.

Um das Fernziel zu erreichen, Metadaten zu erhalten und zu schützen, müssen die folgenden zwei Herausforderungen insbesondere gemeistert werden:

1. Es muss dafür gesorgt werden, dass sich alle Nutzer über die Existenz von Metadaten bewusst sind. Dies kann, neben einer notwendigen Aufklärung, vor allem über eine angemessene Visualisierung der verborgenen Daten geschehen. Es müssen verständliche technische Lösungen geschaffen werden, die Bewusstsein darüber schaffen, was zusammen mit Bildern geteilt wird. Dies gilt für Bilder, die andere im Web teilen oder die ein Nutzer selbst schon im Web geteilt hat, vor allem jedoch auch für die Bilder, die ein Nutzer noch im Web teilen möchte. So bleibt dem Nutzer die Möglichkeit des Eingriffs bevor die Informationen ins Web gelangen und seinen Kontrollbereich verlassen.

2. Es muss den Nutzern auf einfache Weise ermöglicht werden, Metadaten nicht nur zu lassen wie sie sind oder sie vollständig zu entfernen, sondern sie auch partiell zu entfernen und gezielt zu schützen. Die Nutzer müssen selbst entscheiden und steuern können, welche Daten sie mit wem teilen.

6.1 Eine Browser-Erweiterung für die Schaffung von Bewusstsein und die kontrollierte Preisgabe von Bild-Metadaten

Um sich den zwei beschriebenen Herausforderungen anzunehmen, wurde im Rahmen dieser Dissertation die Browser-Erweiterung *Private Foto-Metadaten* für den Webbrowser Chrome entwickelt [157, 103]. Diese schafft Bewusstsein über Metadaten bereits geteilter Bilder mit einem Fokus auf potenziell privatsphärerelevante Informationen. Außerdem bietet sie eine prototypische Umsetzung, die für Bilder, die geteilt werden sollen, Bewusstsein über die eingebetteten Metadaten schafft und außerdem Kontrolle über diese ermöglicht, so dass keine Informationen unbewusst mit einem Bild im Web geteilt werden. Die prototypische Implementierung erlaubt

zudem, Metadaten in einem separaten Metadaten-Dienst zu speichern, um diese gezielt zu schützen.

Die Browser-Erweiterung unterstützt die verbreiteten Metadaten-Standards Exif, IPTC und XMP. Das Lesen und Schreiben aller drei Standards wird durch die Verwendung der C++-Bibliothek *Exiv2* ermöglicht, welche über *Native Client* in die Erweiterung integriert wurde. Um auch eingebettete Personen-Markierungen unterstützen zu können, welche Google Picasa, Windows Live Fotogalerie oder die Apple iOS 7 Kamera-App in Bilder schreiben, wurde Exiv2 um die entsprechenden XMP-Standards erweitert [11].

Existierende Browser-Erweiterungen Im Chrome Web Store existieren verschiedene Browser-Erweiterungen und Apps, die ebenfalls Metadaten von Bildern im Web auslesen und visualisieren können. Diese Erweiterungen, wie beispielsweise *Image-Eigenschaften Kontextmenü*, *Exif Viewer* oder *Send to Jeffrey's Exif Viewer*, sind jedoch vorwiegend für Fotoliebhaber konzipiert, welche aktiv die technischen Details von Bildern betrachten wollen. Keine der Erweiterung hat zum Ziel über privatsphärerelevante Informationen zu informieren, geschweige denn diese gezielt zu visualisieren. Im Gegenteil, einige der zur Verfügung stehenden Erweiterungen erzeugen sogar selbst potenzielle Bedrohungen der Privatsphäre, indem sie die betrachteten Bilder von einem dritten Webdienst verarbeiten lassen, der somit Zugriff auf alle eingebetteten Metainformationen der Bilder erhält. Die hier präsentierte Erweiterung hat einen Fokus auf potenziell privatsphärerelevante Metadaten und verarbeitet alle Informationen direkt im Browser des Nutzers.

6.1.1 Visualisierung von Metadaten

Die Browser-Erweiterung visualisiert Metadaten auf zwei verschiedene Weisen. In der Webseiten-Ansicht signalisieren kleine Indikator-Icons das Vorhandensein von Metadaten in einem Bild. Über das Klicken der Symbole oder über das Kontextmenü eines Bildes kann der Nutzer eine Seitenleiste öffnen, die alle Metadaten eines Bildes im Detail anzeigt. Abbildung 6.1 zeigt exemplarisch eine Foto-Webseite des Dienstes Flickr mit aktivierten Indikator-Icons und der geöffneten Seitenleiste.

Für eine bessere Übersicht und eine effektive Schaffung von Bewusstsein über die privatsphärerelevanten Informationen werden die in einem Bild enthaltenen Metadaten gemäß folgender fünf Informationsarten gruppiert:

- *Personen*: alle identifizierenden Merkmale, beispielsweise Namen abgebildeter Personen, Personen-Markierungen mit und ohne Markierungen im Bild, Name des Fotografen oder des Kamerabesitzers, die eindeutige Seriennummer der Kamera oder des Objektivs

- *Ortsangaben*: alle Ortsangaben, beispielsweise GPS-Koordinaten, textuelle Angaben wie der Name des Aufnahmeortes oder der Name der Stadt
- *Datum & Uhrzeit*: sämtliche Zeit- und Datumsangaben einer Aufnahme
- *Inhaltsbeschreibung*: Informationen wie zum Beispiel der Titel oder die Beschreibung eines Bildes, einfache oder hierarchische Schlagworte
- übrige: alle nicht klassifizierten Informationen inklusive aller technischen Parameter von Kamera und Objektiv

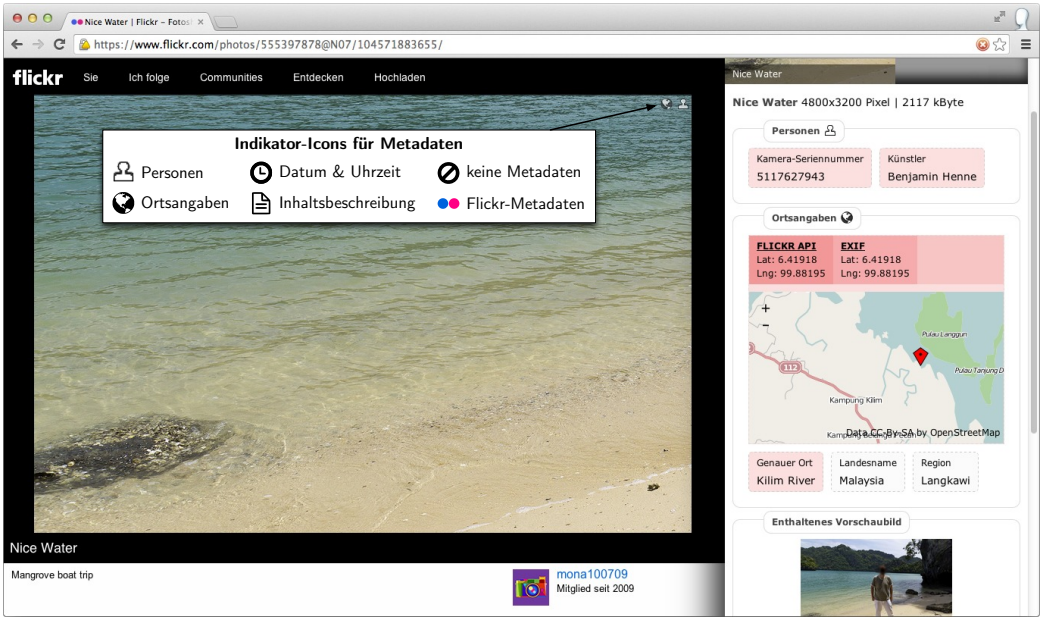


Abbildung 6.1: Eine Foto-Webseite des Dienstes Flickr mit Indikator-Icons und Metadaten-Seitenleiste der Browser-Erweiterung *Private Foto-Metadaten*

Indikator-Icons Damit ein Nutzer auf einen Blick sehen kann, welche Arten von Informationen in einem Bild enthalten sind, können die Schnellindikator-Icons über den Bildern einer Webseite eingeblendet werden. Jede der beschriebenen fünf Gruppen von Metainformationen wird dabei durch ein eigenes Indikator-Icon symbolisiert. Die Anzeige der verschiedenen Indikatoren kann der Nutzer in der Konfiguration beeinflussen. Über ein weiteres Symbol kann zudem angezeigt werden, dass ein Bild gar keine bekannten Metainformationen enthält. Abbildung 6.1 enthält eine Übersicht aller Indikator-Symbole.

Exemplarisch für den Fotodienst Flickr wurde eine gesonderte Unterstützung integriert, die für jeden anderen Dienst mit öffentlicher API implementiert werden kann. Wird ein Foto des Dienstes angezeigt, so werden über die API die öffentlich zugänglichen Metadaten aus der Flickr-Datenbank bezogen und zusammen mit den

eingebetteten Metadaten angezeigt. Das Vorhandensein solcher Metainformationen signalisiert in der Browser-Ansicht ein spezielles Indikator-Icon.

Durch die Indikator-Icons für Metadaten macht die Erweiterung passiv auf das Vorhandensein privatsphärerelevanter Informationen aufmerksam. Dies ermöglicht den Nutzern auf einen Blick zu erkennen, ob potenziell bedrohliche Informationen in einem Bild enthalten sind. Sie müssen somit nicht alle Bilder auf bedrohliche Metadaten hin durchsuchen. Ähnliche Indikatoren aus dem Bereich der IT-Sicherheit haben in der Vergangenheit keinen guten Ruf genossen. Die hier vorgestellte Lösung unterscheidet sich jedoch in zweierlei Hinsicht von diesen: Traditionelle Sicherheitshinweise, wie das grüne Vorhängeschloss für eine sichere SSL-Verbindung, haben meist wenig mit dem eigentlichen Ziel eines Nutzers zu tun [132]. Vielmehr konkurrieren diese Hinweise mit dem Ziel des Nutzers: Der Nutzer will beispielsweise eine Webseite besuchen, der Hinweis gibt jedoch nur Auskunft über die Verbindung, über die sich ein Nutzer meist keine Gedanken machen möchte. Die Metadaten-Indikatoren können effektiver als solche Sicherheitshinweise sein, da die angezeigten Informationen einfach verständlich sind und selbst von direktem Interesse für den Betrachter eines Bildes sein können. Sie weisen ihn auf potenziell private sowie auf nutzbringende Zusatzinformationen zum Bild hin. Sie sind somit mehr Teil des Primärziels als ein Sekundärziel [150]. Sicherheitshinweise wie das Schlosssymbol in der Adressleiste eines Webbrowsers erscheinen zum selben Zeitpunkt wie der Inhalt, der das eigentliche Ziel eines Nutzers ist. Jedoch werden das Schlosssymbol und der Inhalt an verschiedenen Positionen dargestellt, so dass beim Betrachten einer Webseite der Hinweis nicht im Fokus des Nutzers ist. Die Indikator-Icons der beschriebenen Browser-Erweiterung befinden sich hingegen ebenfalls dort, wo auch das Bild abgebildet ist: Sie werden in der oberen rechten Ecke des jeweiligen Bildes angezeigt und befinden sich somit im Fokus des Nutzers, wenn dieser das Bild betrachtet. Zum Vergleich, Maurer et al. [127] hatten gezeigt, dass die Darstellung innerhalb des Bezugskontextes die Effektivität von Warnmeldungen signifikant verbesserte.

Metadaten-Seitenleiste In der Seitenleiste kann sich ein Nutzer die in einem Bild enthaltenen Metainformationen im Detail anzeigen lassen. Über kleine Vorschaubilder am oberen Ende der Leiste kann der Nutzer durch alle Bilder einer Seite navigieren. Wie Abbildung 6.1 zeigt, werden in der Leiste zuerst die Informationen der vier benannten Gruppen dargestellt. Wo es möglich ist, werden dabei die Metadaten visualisiert: GPS-Koordinaten werden auf einer zoombaren Karte dargestellt. Für Personen-Markierungen mit einer Markierung im Bild wird die Markierung im Vorschaubild am oberen Ende der Seitenleiste eingezeichnet (siehe Abbildung 6.9). Schwebt der Nutzer mit dem Mauszeiger über eine solche Markierung, wird der passende Name in Form eines Tooltips angezeigt. Ist ein Vorschaubild in der Bilddatei gespeichert, so wird dieses ebenfalls angezeigt. Dies ermöglicht, verborgene Inhalte

in einem nicht aktualisierten Vorschaubild ausfindig zu machen. Interessierte Nutzer können sich über dies hinaus alle übrigen nicht klassifizierten Metadaten anzeigen lassen, die im Normalfall ausgeblendet sind. Um das Verständnis der enthaltenen Metainformationen zu verbessern, kann sich der Nutzer eine Erklärung zu jedem Eintrag anzeigen lassen.

Da sich die Wahrnehmung der Privatheit der einzelnen Metainformationen zwischen Personen, Generationen oder Kulturen unterscheiden kann, werden die dargestellten Informationen nur nach ihrer inhaltlichen Bedeutung strukturiert und innerhalb einer Gruppe alphabetisch nach ihren Namen sortiert. Die Informationen werden nicht nach einer vorgegebenen Ordnung von Privatheit sortiert. Die Erweiterung ermöglicht dem Nutzer jedoch, einzelne Metainformationen in der Konfiguration als besonders zu markieren, welche daraufhin mit einer vom Nutzer festgelegten Farbe hinterlegt werden können, wie es auch von Shin und Lopes [134] eingesetzt wurde. Dies ermöglicht es den Nutzern die Informationen hervorzuheben, welche ihrem Verständnis nach besonders beachtet werden sollen. Für die im Folgenden vorgestellte Studie wurden einige Informationen als „besonders privat“ markiert und mit der Farbe Rot hinterlegt. Eine mehr nuancierte und wissenschaftlich bestätigte Bewertung und Markierung der Metainformationen sowie der damit erreichte Effekt auf die Nutzer wird im Folgenden nicht betrachtet. Dies sollte jedoch in zukünftigen Arbeiten untersucht werden.

6.1.2 Kontrolle über geteilte Metadaten

Eine Vielzahl von Anwendungen ermöglicht es heute den Nutzern, eingebettete Bild-Metadaten zu verändern oder zu löschen. Solche Software scheint jedoch selten vor dem Hochladen genutzt zu werden. Auch dafür kann das fehlende Bewusstsein über enthaltene Informationen ein Grund sein: Weiß eine Person nicht, dass zusätzliche Kontextinformationen in einem Bild enthalten sind, wird sie auch nicht in Erwägung ziehen, dieses auf eventuelle Bedrohungen ihrer Privatsphäre hin zu untersuchen und zu verändern. Ein anderer Grund für eine geringe Nutzung entsprechender Software kann deren Nutzbarkeit sein: Die meisten Softwarewerkzeuge benötigen ein gewisses Maß an technischem Verständnis. Des Weiteren sind solche Werkzeuge nicht in den regulären Ablauf des Teilens integriert: Ist das primäre Ziel eines Nutzers, ein Bild mit anderen Personen zu teilen, so ist der Nutzer eventuell nicht gewillt den zusätzlichen Aufwand zu investieren, weitere Software im Vorfeld zu verwenden. Eine Ausnahme bilden an dieser Stelle die mobilen Apps *deGeo* (Apple iOS) und *Image Privacy* (Android). Sie ermöglichen Bild-Metadaten beim Teilen zu modifizieren. Jedoch ermöglichen sie nur das Entfernen von GPS-Koordinaten beziehungsweise das uneingeschränkte Löschen aller Exif-Metadaten.

Um diese potenziellen Hinderungsgründe zu adressieren, muss beim Hochladen

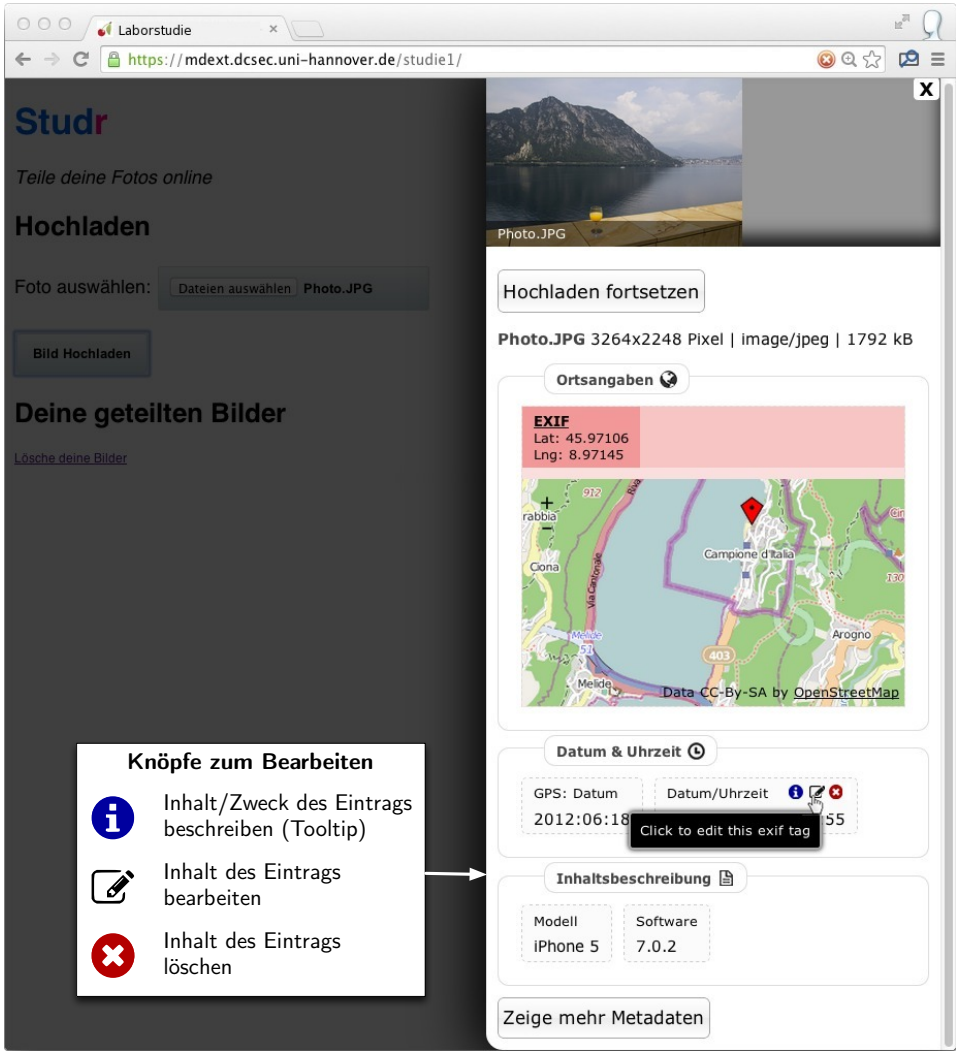


Abbildung 6.2: Seitenleiste zur Bild-Metadaten-Kontrolle beim Hochladen

eines Bildes über einen Webbrowser oder eine App Bewusstsein über die enthaltenen Kontextinformationen geschaffen werden. Außerdem müssen die Nutzer die Möglichkeit haben, im Moment des Teilens die Metadaten zu verändern und teilweise oder vollständig zu löschen. Auf diese Weise erhält der Nutzer die Kontrolle über die enthaltenen Daten, bevor sie im Web preisgegeben werden. In Form einer prototypischen Implementierung wurde dies beides in der Browser-Erweiterung umgesetzt. Aufgrund technischer Beschränkungen[1] funktioniert diese ausschließlich mit einfachen HTML-Formularen. Ist die Kontrollfunktion aktiviert, so überwacht die Erweiterung alle HTML-Formulare auf allen geöffneten Seiten. Wird ein Formular

[1] Die Erweiterung verwendet die *File*-API, *FormData*-API und die *XMLHttpRequest*-API für die Unterbrechung und das erneute Senden. Aufgrund einer Designentscheidung der Chrome-Entwickler ist ein lesender Zugriff auf Dateiinhalte über die *WebRequest*-API nicht möglich. Diese hätte das Abfangen komplexer Uploads (via AJAX et cetera) ermöglicht.

abschickt und enthält Bilddateien zum Hochladen, so unterbricht die Erweiterung das Absenden des Formulars. Die Erweiterung liest die Bilder ein und zeigt sie mit allen eingebetteten Metadaten in der zuvor beschriebenen Seitenleiste an. Wie in Abbildung 6.2 zu sehen ist, ermöglicht die Seitenleiste neben dem Betrachten der Informationen auch das Verändern oder Löschen der enthaltenen Metadaten, was durch die integrierte Exiv2-Bibliothek realisiert wird. Nach dem Betätigen des Knopfes *Hochladen fortsetzen* wird das ursprüngliche Formular mit allen alten Eingaben plus den veränderten Bildern neu erzeugt und abgeschickt.

6.2 Schutz geteilter Metadaten durch Verschlüsselung

Die prototypische Implementierung ermöglicht es Nutzern bewusst zu machen, was sie zusammen mit ihren Bildern im Web teilen. Die Erweiterung erlaubt ihnen, ausgewählte oder alle Metadaten beim Teilen zu löschen. Sollen die nutzbringenden Kontextinformationen jedoch erhalten werden, müssen Wege gefunden werden, um die teils persönlichen Informationen vor unautorisiertem Zugriff zu schützen [103].

6.2.1 Verschlüsselung innerhalb von Bilddateien

Eine theoretisch mögliche Lösung zum Schutz eingebetteter Metadaten ist die verschlüsselte Speicherung der Daten innerhalb der Bilddateien. Dieser Ansatz wäre jedoch mit den verbreiteten Metadaten-Standards nur eingeschränkt möglich und ist als nicht praktikabel angesehen. Da der Metadaten-Standard XMP auf XML und RDF basiert, könnten die gespeicherten Informationen prinzipiell mit Verschlüsselung und auch digitale Signaturen versehen werden, da das Datenformat diese Erweiterung zuließe. Hier lägen weitere Herausforderungen eher im Bereich der Nutzbarkeit. Metadaten der Standards Exif und IPTC werden hingegen als Binärdaten in den Bildern gespeichert. Die Standards definieren strikte Vorgaben für Datenlängen und Typen. Im Falle dieser zwei Standards ist es somit nicht möglich, die Metadaten verschlüsselt in einer Bilddatei zu speichern, ohne die Standards zu verletzen. Alternativ müssten zusätzliche Informationen an einer anderen Position einer Bilddatei gespeichert werden. In diesem Fall wäre es nicht zu verhindern, dass Bildverarbeitungsprogramme die zusätzlichen Informationen ungewollt entfernen.

6.2.2 Metadaten-Dienste

Werden Fotos im Web geteilt, so bietet sich die Speicherung von Metadaten in separaten Metadaten-Diensten aus zweierlei Gründen an. Das Speichern von Metadaten in solch einem Metadaten-Dienst erlaubt das Bewahren und Teilen von Metadaten auch für Fotos, die bei einem Fotodienst hochgeladen werden, der alle Metadaten

aus geteilten Bildern entfernt. Außerdem erlaubt die separate Speicherung von Metadaten auch die Implementierung von Zugriffskontrollen speziell für die Metadaten. Dies ermöglicht unabhängig vom verwendeten Fotodienst, die Bilder und die Metadaten auf verschiedene Weise zu schützen. Auf diese Weise könnten die Metainformationen besser geschützt werden, als es die meisten Dienste heute erlauben.

Um das Konzept eines Metadaten-Dienstes zu evaluieren, wurde ein exemplarisches Testszenario für den Fotodienst Flickr zusammen mit der Browser-Erweiterung implementiert. Flickr wurde gewählt, da für diesen Dienst schon eine spezielle Integration der Flickr-Metadaten implementiert worden war. Eine vergleichbare Anwendung könnte für andere Dienste des Social Webs realisiert werden, die eine öffentliche API für das Teilen von Bildern bereitstellen. Die implementierte Flickr-App ermöglicht Flickr-Nutzern Fotos in ihrem Fotostream zu veröffentlichen und die Metadaten separat zu speichern. Abbildung 6.3 skizziert den Zusammenhang der beteiligten Komponenten: Der Nutzer wird über OAuth gegenüber Flickr authentifiziert und ermöglicht der App mit einem Auth-Token in seinem Namen Fotos hochzuladen. Lädt der Nutzer über die App ein Bild hoch, so öffnet sich der Kontrollmechanismus der Browser-Erweiterung. Der Nutzer kann nun die Metadaten wie beschrieben modifizieren. Beendet er die Bearbeitung wie zuvor beschrieben, so wird das Bild inklusive der Metadaten bei Flickr hochgeladen (1). Alternativ kann er wählen, dass die Metadaten im Metadaten-Dienst gespeichert werden (2a) und das Bild – optional ohne Metadaten – bei Flickr geteilt wird. Für das separate Hochladen der Metadaten werden diese zuvor durch Exiv2 en bloc extrahiert. Betrachtet ein Nutzer später das Foto auf der Flickr-Webseite, so lädt die Browser-Erweiterung die Metadaten von Flickr und vom Metadaten-Dienst und zeigt sie vereint an.

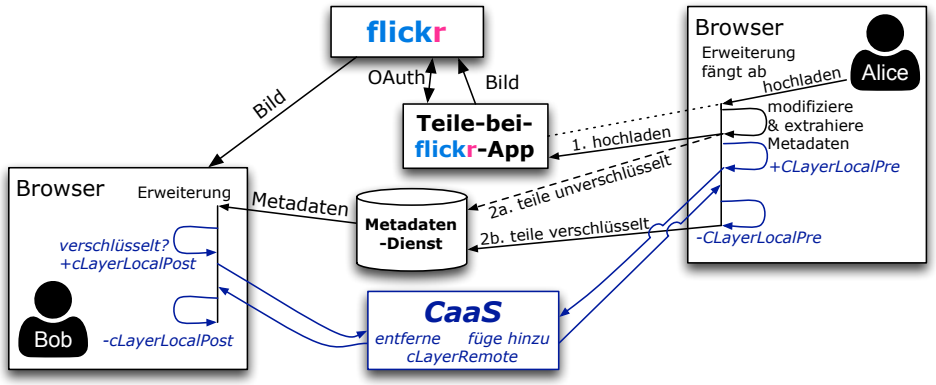


Abbildung 6.3: Konzeptionelle Integration von Browser-Erweiterung, Metadaten-Dienst und CaaS-Provider

6.2.3 Verschlüsselte Speicherung im Metadaten-Dienst

Um keine Bedrohungen für die Privatsphäre durch die im Metadaten-Dienst gespeicherten Informationen entstehen zu lassen, kann neben Zugriffskontrollmechanismen auch Verschlüsselung eingesetzt werden. Um die Metadaten vor jeglichem Missbrauch zu schützen, sollten sie so verschlüsselt werden, dass weder der Dienstanbieter noch andere unautorisierte Personen Zugriff auf die ungeschützten Daten erlangen können. Durch die Speicherung der Metadaten im Dienst wird eine Verschlüsselung erleichtert, da die zuvor beschriebenen Einschränkungen durch die Metadaten-Standards nicht gegeben sind. Um die Komplexität des Schutzes nicht über das notwendige Maß hinaus wachsen zu lassen, bietet es sich für ein einfaches System an, alle Metadaten en bloc zu verschlüsseln, wie sie zuvor auch extrahiert wurden.

Das grundlegende Problem vieler Verschlüsselungslösungen ist, dass die Verwaltung der verwendeten Schlüssel den Nutzern so viele Schwierigkeiten bereitet, dass diese sich nicht die Mühe machen, Verschlüsselung zu verwenden, oder sie falsch verwenden [151, 97, 133]. Für den hier präsentierten Anwendungsfall bietet sich daher das *Confidentiality as a Service*-Paradigma (CaaS) von Fahl et al. [92] an, um die gespeicherten Metadaten zu verschlüsseln. Die gute Nutzbarkeit des Ansatzes wurde schon im Kontext der Verschlüsselung von Facebook-Nachrichten gezeigt [93]. CaaS benötigt keine Verwaltung von Schlüsseln durch den Nutzer. Nutzer müssen sich lediglich per E-Mail und Passwort authentisieren. CaaS verteilt das notwendige Vertrauen auf den Metadaten-Dienst und einen CaaS-Dienst. Durch die Verwendung kommutativer Ebenen symmetrischer Verschlüsselung erhält weder der CaaS-Dienst noch der Metadaten-Dienst Zugriff auf die unverschlüsselten Metadaten. Wie folgt würde die Anwendung des CaaS-Paradigmas im Anwendungsfall des Metadaten-Dienstes vonstattengehen: Wählt ein Nutzer die Verschlüsselung seiner Metadaten für den Metadaten-Dienst, so gibt er beim Fortsetzen des Hochladens zusätzlich das Publikum der Metadaten und sein CaaS-Passwort an. Ist das Publikum *öffentlich*, so werden die Metadaten unverschlüsselt beim Metadaten-Dienst gespeichert (Abbildung 6.3: 2a). Andernfalls wählt der Nutzer aus seiner Kontaktliste diejenigen aus, die die Metadaten entschlüsseln und betrachten dürfen, und definiert so die Zugriffsliste für die CaaS-Verschlüsselung. Wählt der Nutzer eine Gruppe von Personen wie *Familie* oder *Freunde* aus, so wird jede Person, die sich in dieser Gruppe befindet, automatisch hinzugefügt. Dabei erlaubt CaaS nur solche Nutzer in die Zugriffsliste aufzunehmen, die dem Dienst schon bekannt sind, da sonst Sicherheitsprobleme entstehen könnten. Die Browser-Erweiterung verschlüsselt die Metadaten lokal und schickt diese an den CaaS-Dienst. Nachdem dieser die Metadaten ebenfalls verschlüsselt hat und die Browser-Erweiterung die lokale Verschlüsselung wieder entfernt hat, werden die Metadaten mit der Verschlüsselung des CaaS-Dienstes im Metadaten-Dienst gespeichert (2b). Besucht ein Nutzer eine Webseite mit einem

Foto, für das Metadaten im Metadaten-Dienst hinterlegt worden sind, lädt die Erweiterung die Metadaten. Sind die Metadaten verschlüsselt und steht der Nutzer auf der dazugehörigen Zugriffsliste, so werden die Metadaten unter der Verwendung des eingegebenen CaaS-Passworts entsprechend entschlüsselt, und wie beschrieben von der Browser-Erweiterung verwendet.

6.3 Laborstudie zur Evaluierung der Browser-Erweiterung

Um die Nutzbarkeit der Browser-Erweiterung und den Gewinn für die Nutzer zu evaluieren, wurde eine Laborstudie durchgeführt [103].

6.3.1 Durchführung und Demographie

Um Teilnehmer für die Studie zu rekrutieren, wurden 1.500 Abonnenten des E-Mail-Verteilers für Studien und Umfragen zu Forschungsthemen der Arbeitsgruppe Distributed Computing & Security angeschrieben. Eingeladen wurde zu einer „Nutzerstudie zum Teilen von Fotos im Web“. 62 Personen füllten daraufhin den Online-Fragebogen aus, der die Studie vorstellte und der Planung der Labortermine diente. Außerdem sammelte der Fragebogen demographische Informationen und Selbsteinschätzungen der Nutzer zu ihrem Wissen über Metadaten. Der vollständige Fragebogen ist inklusive der Häufigkeiten der Antworten in Anhang C.3 zu finden.

69,4 % der 62 Teilnehmer wählten die korrekte Definition des Begriffs der Metadaten aus den vier gegebenen Möglichkeiten. 51 % der Teilnehmer, die zu Wissen zeigten, was Metadaten sind, gaben an, nicht zu wissen, welche zusätzlichen Informationen sie zusammen mit ihren Bilder teilen. 58 % von ihnen gaben an, nicht zu wissen, was die von ihnen verwendeten Fotodienste mit den enthaltenen Zusatzinformationen machen. 32 % gaben an, sich keine Gedanken über enthaltene Metadaten zu machen, wenn sie Bilder teilen. 9 % von denen, die Metadaten korrekt definierten, gaben an, alle Metadaten aus Bildern zu löschen, bevor sie diese teilen. Zusätzliche 16 % gaben an, die Metadaten teilweise zu löschen. Vergleicht man die Werte mit denen aus Abschnitt 5.3, ist der Anteil derer, die den Begriff der Metadaten korrekt definierten, hier etwas höher. Hingegen gaben weniger Teilnehmern an, sich über die Verwendung von Metadaten bewusst zu sein und Metadaten zu modifizieren.

Alle 62 Teilnehmer des Fragebogens wurden zur Laborstudie eingeladen. 43 von ihnen nahmen an der Laborstudie teil und beendeten die Aufgaben vollständig. Alle Teilnehmer waren Studierende oder Bedienstete der Leibniz Universität Hannover. 62,8 % von ihnen waren weiblich und 37,2 % waren männlich. Das durchschnittliche Alter der Teilnehmer betrug 24 ± 4 Jahre. Für die Teilnahme an der Studie erhielt jeder Teilnehmer eine Aufwandsentschädigung von 5 Euro. Im Vorfeld wurden alle

Teilnehmer gebeten, für eine höhere Realitätsnähe der Ergebnisse ein Bild bereitzustellen, dass sie mit ihrer Digitalkamera oder ihrem Kamera-Handy gemacht hatten. Die Studie wurde in 15 Sitzungen an zwei Tagen mit Gruppen von bis zu 6 Personen durchgeführt. Nach einer mündlichen Begrüßung wurden die Teilnehmer durch eine grobe schriftliche Aufgabenbeschreibung durch die Studie geleitet und beantworteten im Rahmen der praktischen Aufgaben 22 Fragen auf einem Papier-Fragebogen. Das verwendete Studienmaterial ist in Anhang C.3 zu finden.

Während es viele Mittel und Wege gibt, neue Funktion zur Wahrung der IT-Sicherheit und Privatsphäre zu untersuchen, ist es eine wiederkehrende grundlegende Entscheidung, ob die Teilnehmer über den Gegenstand der Untersuchung im Vorfeld aufgeklärt werden. Da die Entwicklung der Browser-Erweiterung noch in den Anfängen steckte und es Ziel der Studie war, Rückmeldungen zur Nutzbarkeit der erstellten Nutzerschnittstelle zu bekommen sowie zum Interesse der Nutzer an den neuen Funktionen, wurden die Teilnehmer in dieser Laborstudie offen darüber aufgeklärt, was untersucht wird. Von den vier untersuchten Aspekten, den Metadaten-Indikatoren, der Seitenleiste, der Modifikation von Metadaten beim Hochladen und der Verschlüsselung, betraf dies vorwiegend die Indikatoren. Ohne eine vorherige Einführung müssten diese von den Teilnehmern erst wahrgenommen werden, bevor sie ihnen nutzen. Da das Hauptanliegen war, herauszufinden, ob die Teilnehmer generell daran interessiert sind, ihre eigenen Metadaten zu kennen und zu kontrollieren, war das Prüfen der Sichtbarkeit der Indikatoren nicht im Fokus der Studie.

Die Teilnehmer wurden in der Begrüßung darüber aufgeklärt, dass die Laborstudie dazu diene, zwei neue Funktionen des Webbrowsers Chrome zum Schutz der Privatsphäre zu untersuchen: Die Möglichkeit Metadaten beim Hochladen zu verändern oder zu löschen und eine Metadaten-Anzeige kombiniert mit Hinweis-Icons in der Webseiten-Ansicht. Der Herstellername Google wurde in der Laborstudie vermieden, um eine Beeinflussung durch eine eventuelle negative Konnotation des Firmennamens zu vermeiden. Die Teilnehmer wurden nicht darüber aufgeklärt, wer die Autoren der Browser-Erweiterung waren. Sie wurden in dem Glauben gewogen, dass es sich um unveröffentlichte Funktionen des Webbrowsers handele, die untersucht werden sollen. Durch diese Herangehensweise sollte eine Beeinflussung der Ergebnisse vermieden werden, die entsteht, wenn Teilnehmer den Autoren einer evaluierten Software mit ihren Antworten einen Gefallen tun wollen.

Diskussion empirischer Daten Neben dem Modus der Antworten werden im Folgenden vorwiegend Durchschnittswerte der Antworten $\varnothing$ und die dazugehörigen Standardabweichungen s beschrieben. Da die Antworten der Teilnehmer statistisch signifikante Abweichungen von der Normalverteilung zeigten, werden für die Analyse der Ergebnisse nicht-parametrische Tests verwendet.

6.3.2 Bewusstsein und Kontrollgefühl der Nutzer

Zu Beginn der Laborstudie wurden die Studienteilnehmer gefragt, inwieweit sie sich Gedanken darüber machen, ob/wo/wie sie im Web persönliche Informationen preisgeben. Auf der 5-Punkte-Skala von *(1) gar nicht* bis *(5) sehr stark* antworteten die Teilnehmer der Laborstudie mit einem durchschnittlichen Wert von 4 ($s = 0{,}9$, Modus = 4), wobei 9 % der Antworten auf die unteren zwei Werte entfielen. Außerdem wurden sie gebeten einzuschätzen, wie sehr sie die Kontrolle darüber haben, was sie von sich preisgeben, wenn sie Fotos im Web teilen. Auf der 5-Punkte-Skala von *(1) gar nicht* bis *(5) voll und ganz* gaben die Teilnehmer für ihr Kontrollgefühl einen durchschnittlichen Wert von 2,7 ($s = 1$) an, wobei 20 % der Antworten auf die unteren zwei Werte entfielen. Die Antworten der Teilnehmer zeigten einen deutlichen gefühlten Mangel an Kontrolle, den die Browser-Erweiterung versucht zu verringern.

6.3.3 Bewusstsein und Kontrolle beim Hochladen

Im ersten praktischen Teil der Laborstudie wurden die Teilnehmer angeleitet, fünf Fotos auf einer für die Studie erstellten Seite hochzuladen. Zu aller erst luden sie ein Foto ohne Metadaten hoch, in dessen Fall die Browser-Erweiterung die Seitenleiste nicht öffnete und das Hochladen wie gewohnt vonstattenging. Als Nächstes wurden sie gebeten ihr selbst gemachtes Foto hochzuladen, welches sie zuvor bereitgestellt hatten. Diejenigen, die dies nicht oder zu spät getan hatten, wurden gebeten eines von zwei Ersatzfotos hochzuladen, dass mit dem von ihnen bevorzugten Mobiltelefon geschossen wurde: ein Foto eines aktuellen iPhones (mit eingebetteter GPS-Ortsangabe und einer nicht benannten Personen-Markierung) oder ein Foto eines Android-Telefons (mit GPS-Ortsangabe). 20 % der Teilnehmer griffen auf ihr bereitgestelltes Foto zurück, deren Metadaten von rein technischen Informationen bis zu den GPS-Koordinaten der Wohnung einer Teilnehmerin reichten. Die übrigen 80 % wählten jeweils ein anderes Fotos. Zuletzt luden die Teilnehmer drei weitere Fotos mit verschiedenen Metadaten hoch, deren Reihenfolge auf Basis des lateinischen Quadrats gleichmäßig über die Teilnehmer verteilt wurde, um Beeinflussungen durch die Reihenfolge der Bilder auszugleichen: ein Partyfoto einer namentlich benannten Studentenparty mit mehreren deutlich erkennbaren Gesichtern, von denen eines mit Namen annotiert war; ein Foto eines hochwertigen Fahrrads vor dem Hauptgebäude der Universität inklusive des Namens des Kamerabesitzers und der eindeutigen Seriennummer der Kamera; ein Foto eines heimischen Esstisches im Kerzenschein mit GPS-Koordinaten irgendwo in einem universitätsnahen studentischen Wohnviertel.

Nachdem die Teilnehmer ihr eigenes Foto oder ein Ersatzfoto hochgeladen hatten, und dadurch erstmals der Hochladen-Seitenleiste und den im Bild enthaltenen Metadaten begegnet waren, wurden sie gefragt, ob sie wussten, dass solche Informationen in (ihren) Bildern gespeichert sind. 19 % von ihnen antworteten mit *Nein*,

23 % antworteten mit *Ja* und 58 % antworteten, sie hätten gewusst, dass Informationen enthalten sind, jedoch nicht welche. 20 % deren, die mit Ja antworteten, gaben später in der Studie an, über manche Arten von Informationen jedoch verwundert gewesen zu sein. Dieses Ergebnis betont, dass selbst wenn die Nutzer wissen, was Metadaten im Allgemeinen sind, die meisten von ihnen nicht wissen, was tatsächlich in Fotos enthalten ist und mit ihnen geteilt wird.

Nach dem Hochladen aller fünf Fotos wurden die Teilnehmer gefragt, inwieweit die neue Funktion ihr Wissen darüber verbessert, was sie mit ihren Fotos teilen. Auf der 5-Punkte-Skala von *(1) gar nicht* bis *(5) sehr stark* antworteten die Teilnehmer mit dem durchschnittlichen Wert von 4,5, wobei 69 % von ihnen mit *sehr stark* antworteten. Dies ist ein deutliches, sehr motivierendes Ergebnis. Obwohl die Teilnehmer informiert worden waren, was untersucht wird, und sie sich so schon gedanklich mit dem Thema der verborgenen Daten beschäftigt hatten, fanden sie die Funktion äußerst aufschlussreich. Als Nächstes wurde die gleiche Frage in Bezug auf die Kontrolle, was mit Bildern geteilt wird, gestellt. Die Teilnehmer beantworteten diese mit einem durchschnittlichen Wert von 4,3, wobei 55 % von ihnen mit *sehr stark* antworteten. Abbildung 6.4 zeigt die Verteilung der Antworten beider Fragen. Ein einzelner Teilnehmer kommentierte im Fragebogen, dass er trotzdem das Gefühl habe, keinen Überblick zu haben, was er alles im Web teilt. Ein Großteil der Teilnehmer gab jedoch an, dass die neue Funktion ihr Bewusstsein und ihre Kontrolle über die geteilten Informationen verbessert.

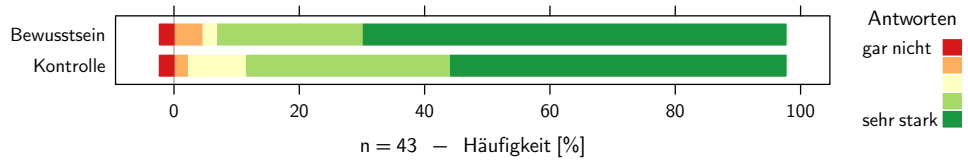


Abbildung 6.4: Wahrgenommene Verbesserung von Bewusstsein und Kontrolle durch die Hochladen-Seitenleiste

In dieser praktischen Aufgabe, in der die Nutzer die Seitenleiste zum Betrachten und Verändern der enthaltenen Metadaten erstmals sahen und ihnen freigestellt war, die Funktionen zu verwenden, löschten 11 Teilnehmer ausgewählte Metadaten von durchschnittlich 2,4 Fotos. 15 Teilnehmer verwendeten die Funktion *Alle Metadaten Löschen* bei durchschnittlich 2,5 anderen Fotos, wobei 9 von ihnen erst vereinzelte Informationen löschten, zuletzt jedoch alle löschten. Als die Teilnehmer am Ende der Laborstudie gefragt wurden, ob und warum sie Metadaten im Rahmen dieser Aufgabe gelöscht hatten (42 % bejahten das Löschen), erklärten einige, dass sie keine Metadaten gelöscht hätten, da es nur eine Studie gewesen sei oder es nicht ihre eigenen Fotos waren. Interessanterweise gab eine Teilnehmerin an, Metadaten gelöscht zu haben, weil sie keine Informationen über andere preisgeben wolle, die sie selbst als privat empfinde, selbst wenn sie die betroffenen Personen nicht kennt. Dies war

eine positive Überraschung, da dieser Aspekte von der Studie gar nicht betrachtet werden sollte. Er sollte jedoch bei der weiteren Entwicklung von Werkzeugen wie der Browser-Erweiterung berücksichtigt werden.

Nach der Benutzung der Hochladen-Seitenleiste wurde die Wahrnehmung der Teilnehmer über die Erstnutzung und die generelle Nutzbarkeit der Erweiterung erfasst. Sie wurden nach dem ersten Nutzen der Seitenleiste gefragt, inwieweit sie meinen die neue Funktion auf Anhieb verstanden zu haben. Auf der 5-Punkte-Skala von *(1) gar nicht* bis *(5) voll und ganz* beantworteten sie die Frage mit einem durchschnittlichen Wert von 3,8 ($s = 1{,}1$).

Nach dem Hochladen aller Bilder wurden die Teilnehmer gefragt, wie sie die Integration des Bearbeitens/Löschens direkt beim Hochladen von Fotos finden. Auf der 5-Punkte-Skala von *(1) unpraktisch/hinderlich* bis *(5) äußerst praktisch/sehr gut* antworteten sie im Durchschnitt mit dem Wert 4,3. 58 % der Antworten entfielen dabei auf die positivste Antwort und 5 % auf die unteren zwei. Die Teilnehmer wurden außerdem gefragt, wie häufig sie die neuen Funktionen auch in ihrem Browser zuhause nutzen wollen würden. Ihre Antworten gaben sie auf der 5-Punkte-Skala von *(1) nie* über *(3) ab und zu* bis *(5) immer*. Abbildung 6.5 zeigt die Verteilung der Antworten. Im Fall der Anzeige der enthaltenen Metadaten antworteten sie mit dem durchschnittlichen Wert von 4,2 ($s = 1$, Modus = 5). In Bezug auf die Möglichkeit Metadaten zu entfernen war die durchschnittliche Antwort der Wert 4 ($s = 1$, Modus = 5). Im Gegensatz dazu wurde die Möglichkeit Daten zu verändern nur mit einem durchschnittlichen Wert von 3,7 ($s = 1{,}1$, Modus = 4) beantwortet. Die Teilnehmer bevorzugten die Anzeige signifikant gegenüber dem Modifizieren (Wilcoxon-Test: $z = -3$, $p < 0{,}05$). Das Löschen bevorzugten sie sichtbar gegenüber der Modifikation (Wilcoxon-Test: $z = -1{,}7$, $p = 0{,}08$).

Auf die Frage nach fehlenden Funktionen hin wünschten sich einige Teilnehmer einfacheres Löschen ganzer Gruppen von Informationen, beziehungsweise eine Standardeinstellung alle Metadaten zu löschen. Andere wünschten sich, Informationen zu Bildern hinzufügen zu können: Sie würden beispielsweise Personen-Markierungen, Ortsangaben oder einen Copyright-Vermerk vor dem Teilen hinzufügen wollen. Ein Teilnehmer wünschte sich, Metadaten verschlüsseln zu können.

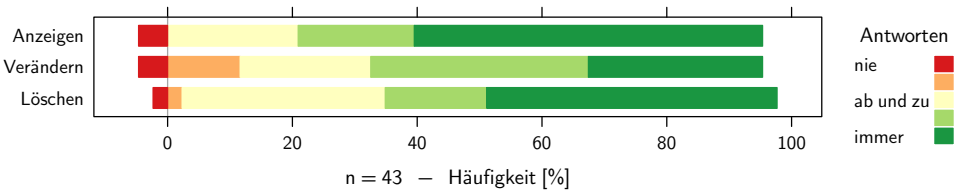


Abbildung 6.5: Willen, die neuen Hochladen-Funktionen zukünftig zu nutzen

Am Ende der Aufgabe wurden die Teilnehmer gebeten, die Nutzbarkeit der erprobten Funktion zu bewerten. Hierzu wurde der *System-Usability-Scale*-Fragebogen

verwendet um die *SUS-Score* [79] für die Hochladen-Seitenleiste zu bestimmen. Die Bewertung ergab eine durchschnittliche SUS-Score von 73,5 von 100 Punkten. Dies bescheinigt eine gute Nutzbarkeit.

6.3.4 Bewusstsein über Metadaten im Web

Im zweiten praktischen Teil der Laborstudie wurden die Teilnehmer angeleitet, sich Metadaten von Fotos im Web anzuschauen. Um vergleichbare Ergebnisse zu erzielen, wurden die Teilnehmer dazu anfangs auf eine vorbereitete Webseite gelotst. Diese Seite zeigte vier Bilder aus dem Web inklusive Weblinks zu den Originalseiten: ein Gruppenfoto der Arbeitsgruppe Distributed Computing & Security mit Ortsangabe der Universität, dem Namen des Kamerabesitzers und der Seriennummer der Kamera; ein Flickr-Foto eines Kindes mit Personen-Markierung mit dem vollständigen Namen des Kindes; ein Flickr-Foto eines Vaters mit zwei Kindern zuhause mit GPS-Koordinaten; ein Foto eines jungen Mädchens, das vor einem Spiegel posiert – das Gesicht war im Bild abgeschnitten doch die eingebettete Vorschau zeigte es. Außerdem enthielt die vorbereitete Webseite einen Link zur Seite der aktuell hochgeladenen iPhone-4S-Fotos bei Flickr sowie einen Link zur öffentlichen Foto-Community *fotocommunity.de*, die ebenfalls Metadaten geteilter Fotos erhält.

Den Teilnehmern war freigestellt zu entscheiden, welche Bilder und Metadaten sie wie lange betrachten. Im Durchschnitt besuchten sie drei verlinkte externe Seiten und betrachteten die Metadaten von vier Bildern in der Seitenleiste über eine Zeitspanne von grob fünf Minuten. Nachdem die Teilnehmer selbst entschieden hatten, die Funktion ausreichend erprobt zu haben, beantworteten sie die folgenden Fragen zu den verschiedenen Visualisierungsfunktionen. Die Teilnehmer wurden gefragt, wie hilfreich die Hinweis-Icons auf den Bildern für die Übersicht sind, was für Informationen in den Bildern enthalten sind. Auf der 5-Punkte-Skala von *(1) gar nicht hilfreich* bis *(5) äußerst hilfreich* gaben sie eine durchschnittliche Antwort vom Wert 4,1 (s = 1,1 , Modus = 5). Nur 9 % der Antworten entfielen auf die zwei schlechtesten Antwortmöglichkeiten. Die Teilnehmer wurden ebenfalls gefragt, wie stark sie die Hinweis-Icons beim Surfen stören. Auf der 5-Punkte-Skala von *(1) stören gar nicht* bis *(5) stören sehr* gaben sie eine durchschnittliche Antwort vom Wert 1,5 (s = 0,7). Nur einer von ihnen wählte eine der zwei höchsten Antworten. Die meisten Teilnehmer nahmen die Indikator-Icons als hilfreich bis zu sehr hilfreich war und kaum jemand fühlte sich von ihnen gestört. Diese Bewertung fand jedoch im Fokus der gestellten Aufgabe statt und nicht beim alltäglichen Surfen im Web. Besonders die Frage nach der Störung muss noch genauer in einer Feldstudie evaluiert werden. Dies sollte natürlich erst geschehen, wenn die Nutzbarkeit der Browser-Erweiterung bewertet worden ist und darauf basierend insoweit verbessert wurde, dass die Software in einer Feldstudie erprobt werden kann.

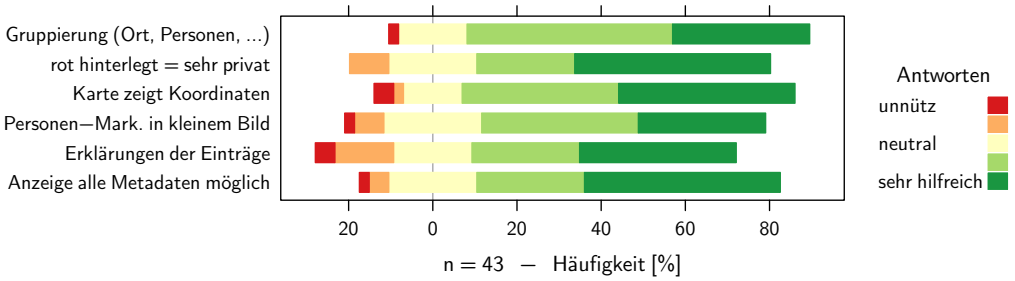


Abbildung 6.6: Wahrnehmung der verschiedenen Visualisierungsfunktionen für Metadaten

Da die Seitenleiste verschiedene Aspekte vereinte, die das Verständnis der enthaltenen Metadaten und der daraus resultierenden Bedrohungen fördern sollten, wurden die Teilnehmer gefragt, wie sie diese wahrnehmen. Abbildung 6.6 zeigt die Bewertung der einzelnen Aspekte auf der 5-Punkte-Skala von *(1) unnütz* bis *(5) sehr hilfreich* mit *(3) neutral*. Die Gruppierung von Informationen, die rote Markierung sehr privater Informationen, die Visualisierung von Koordinaten auf einer Karte und die Möglichkeit alle Metadaten anzeigen zu lassen wurden von den Teilnehmern mit einem durchschnittlichen Wert von 4,1 ($s = 1$, Modus = 5) bewertet. Die Anzeige von Personen-Markierungen im verkleinerten Bild am oberen Ende der Seitenleiste bewerteten sie durchschnittlich mit dem Wert 3,9 ($s = 1$, Modus = 4). Die Tooltip-Einblendung von Erklärungen der einzelnen Metainformationen bewerteten sie im Durchschnitt mit dem Wert 3,8 ($s = 1{,}2$, Modus = 5). Keine der Visualisierungsfunktionen wurde als nutzlos betrachtet. Im Fall der Erklärungen waren 18 % der Bewertungen schlechter als neutral. In allen anderen Fällen waren es unter 10 %.

Um den Gewinn an Bewusstsein zu erfassen, wurden die Teilnehmer gefragt, inwieweit die erprobte Funktion ihnen hilft, einen besseren Überblick darüber zu haben, was alles in Bilder gespeichert ist, die sie und andere im Web teilen. Abbildung 6.7 zeigt ihre Antworten auf der 5-Punkte-Skala von *(1) hilft gar nicht* bis *(5) hilft sehr gut*. Der Durchschnitt ihrer Antworten war der Wert 4,6 ($s = 0{,}8$, Modus = 5), was eine beträchtliche Verbesserung bezeichnet.

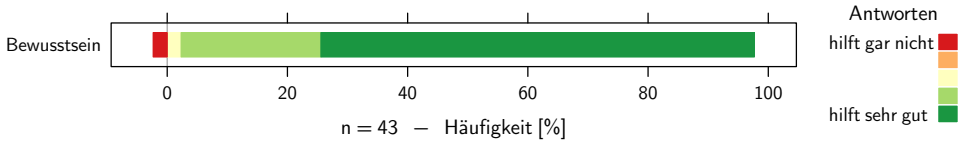


Abbildung 6.7: Wahrgenommene Verbesserung des Bewusstseins über geteilte Metadaten

Auch bei dieser Funktion wurden die Teilnehmer gefragt, wie häufig sie diese zuhause nutzen wollen würden. Ihre Antworten auf der 5-Punkte-Skala von *(1) nie* bis *(5) immer* mit *(3) ab und zu* zeigt Abbildung 6.8. Über 60 % der Antworten entfielen auf die Antworten häufiger als ab und zu bis immer. Niemand antwortete *nie*. Die Antworten lassen vermuten, dass die Teilnehmer die Indikator-Icons mit

einem mittleren Wert von 4,2 ($s = 0{,}9$, Modus = 5) gegenüber der Ansicht in der Seitenleiste mit einem mittleren Wert von 4 ($s = 1$, Modus = $\{4, 5\}$) leicht bevorzugen (Wilcoxon-Test: $z = 1{,}7$, $p = 0{,}09$).

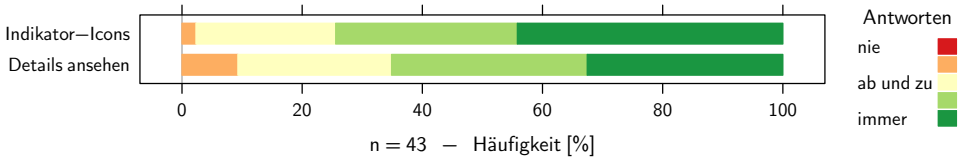


Abbildung 6.8: Willen, die neuen Visualisierungsfunktionen zukünftig zu nutzen

Am Ende der Aufgabe wurden die Teilnehmer gebeten, die Nutzbarkeit der nun erprobten Funktion zu bewerten. Die Bewertung der Visualisierungsfunktionen ergab eine durchschnittliche SUS-Score von 76,9 von 100 Punkten. Dies bescheinigt abermals eine gute Nutzbarkeit.

6.3.5 Schutz und Nutzen von Metadaten

Im dritten praktischen Teil der Laborstudie wurden die Teilnehmer angeleitet, ihr eigenes oder eines der zwei Ersatzfotos noch einmal hochzuladen. Um zu evaluieren, ob sie fähig wären, eine CaaS-basierte Verschlüsselung von Metadaten zu nutzen und um zu erfassen, ob sie Interesse an der Verschlüsselung hätten, wurde in diesem Fall eine modifizierte Version der Seite zum Hochladen verwendet, die das Speichern der Metadaten in einem Metadaten-Dienst unterstützt. In die Browser-Erweiterung wurde außerdem eine Mock-up-Implementierung der CaaS-Verschlüsselung integriert, die auf dieser Seite automatisch aktiviert wurde. Beim Hochladen des Fotos wurden den Teilnehmern in diesem Fall zwei Köpfe zum Fortsetzen des Hochladens angezeigt, wie in Abbildung 6.9 zu sehen ist: *Hochladen fortsetzen* und *Hochladen fortsetzen; Metadaten verschlüsseln*. Beim Betätigen des Knopfes zum Verschlüsseln wurden die Metadaten aus der Bilddatei entfernt und im Metadaten-Dienst gespeichert. Der Teilnehmer wurde in diesem Fall gebeten Kontakte aus seiner Rollenspiel-Kontaktliste zu wählen, die neben einigen Personennamen die Gruppen *Familie* und *Freunde* sowie die Sonderauswahl *nur ich* enthielt. Daraufhin musste der Teilnehmer sein CaaS-Passwort eingeben und das Bild und die Metadaten wurden hochgeladen. Beim Neuladen der Seite nach dem Hochladen wurde das neue Bild in der Liste der geteilten Bilder angezeigt. Die Browser-Erweiterung erkannte, dass zu diesem Bild externe Metadaten vorlagen, empfing diese, fragte nach dem CaaS-Passwort des Teilnehmers, entschlüsselte die Metadaten und zeigte sie für das Bild wie gewohnt an. Für folgende Aktionen wurde das Passwort im Cache der aktuellen Browser-Session gespeichert, wie es der CaaS-Workflow vorsieht [93].

Während die Teilnehmer darüber informiert wurden, dass sie bei dieser Aufgabe ein bekanntes Bild mit Metadaten hochladen, ging die Aufgabenbeschreibung nicht

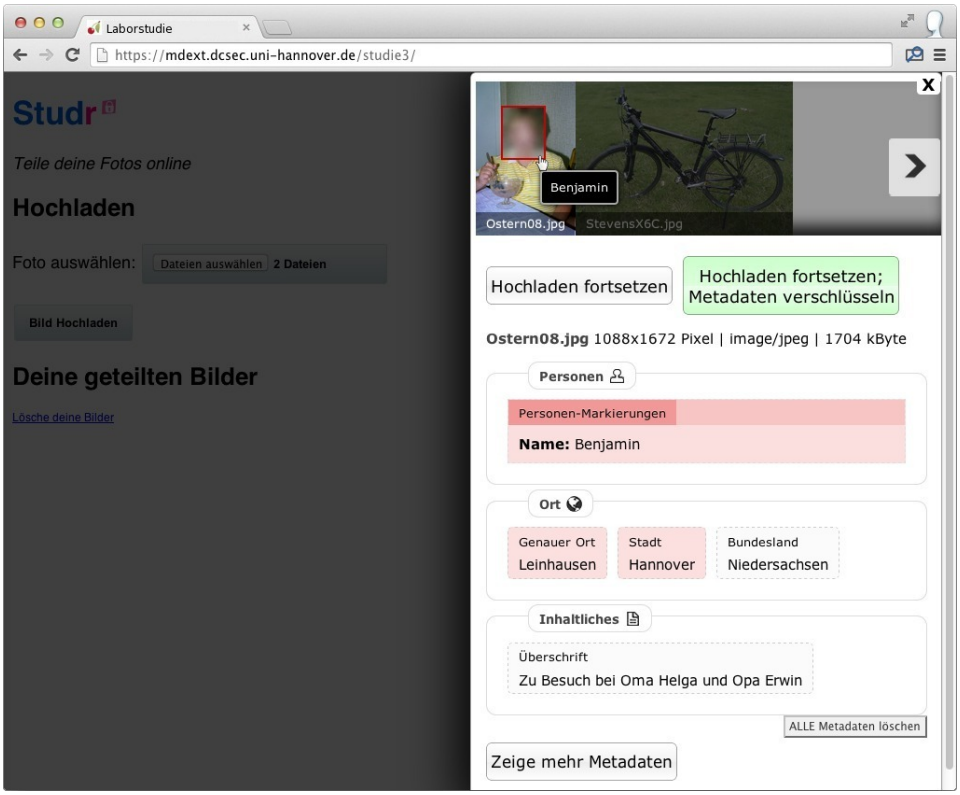


Abbildung 6.9: Seitenleiste zur Bild-Metadaten-Kontrolle beim Hochladen mit der Option Metadaten zu verschlüsseln und der Visualisierung einer Personen-Markierung

weiter auf die mögliche Verschlüsselung ein. Die Aufgabenbeschreibung gab lediglich ein Passwort an, dass die Teilnehmer verwenden sollten, falls sie eines benötigen. Sie wurden nicht instruiert die Verschlüsselung zu verwenden. In der Laborstudie verschlüsselten 56 % der Teilnehmer eigenständig die Metadaten beim Hochladen.

Im Fragebogen wurden die Teilnehmer gefragt, ob sie Metadaten als *(1) Bedrohung der Privatsphäre* oder als *(5) nützlich und sinnvoll* empfinden. Auf der gegebenen 5-Punkte-Skala gaben sie im Durchschnitt an, Metadaten als Bedrohung zu sehen ($\varnothing = 1{,}7$, $s = 1$, Modus = 1), wenn sie Bilder im Web teilen. Für den Fall, dass sie Bilder mit einer einzelnen Person teilen, beispielsweise über eine E-Mail, bewerteten sie Metadaten als eher nützlich und sinnvoll mit einem durchschnittlichen Wert von 3,9 ($s = 1$, Modus = 4). Für den privaten Gebrauch bewerteten sie Metadaten im Durchschnitt als nützliche und sinnvolle Informationen ($\varnothing = 4{,}6$, $s = 0{,}9$, Modus = 5).

Am Ende dieser Aufgabe wurden die Teilnehmer gebeten zu bewerten, welche Wege zum „Schutz“ von Metadaten sie persönlich bevorzugen würden. Abbildung 6.10 zeigt das vollständige Ranking der verschiedenen Maßnahmen. An erster Stelle gaben 40 % der Teilnehmer an, das vollständige Löschen von Metadaten zu präferieren. 33 % der Teilnehmer gaben an, stattdessen die Verschlüsselung von Metadaten vorzuziehen. Dies ist ein überraschendes Ergebnis, wenn man bedenkt, wie unpopulär

Verschlüsselung beispielsweise in der E-Mail-Kommunikation ist. Da die Teilnehmer im Rahmen ihrer Aufgaben keine Metadaten verschlüsseln mussten, war es nicht zu erwarten, das so viele Personen Verschlüsselung als erste Wahl angaben. Andere 26 % der Teilnehmer gaben als erste Wahl an, einige Metadaten zu entfernen, bevor sie Bilder öffentlich teilen. Ein einziger Teilnehmer gab an, Bilder so zu teilen, wie sie sind. Dieser eine Nutzer wählte damit als Präferenz das, was heute gängige Praxis ist. In einem Gespräch nach der Studie sprach er sich dafür aus, dass alle Nutzer noch viel mehr Metadaten zu Bildern hinzufügen sollten. An zweiter Stelle gaben 53 % der Teilnehmer an, ausgewählte Metadaten zu löschen. 23 % von ihnen wählen die Verschlüsselung und 19 % wählen das vollständige Löschen aller Metadaten. Bilder mit unveränderten Metadaten zu teilen war die letzte Wahl von insgesamt 86 % der Studienteilnehmer. Die Antworten der Teilnehmer zeigen den deutlichen Wunsch, Metadaten vor der unkontrollierten Preisgabe zu schützen. Zu einem nennenswerten Teil zeigen sie auch den Wunsch, die Metainformationen zu verschlüsseln, was ermöglicht, die Informationen zu schützen und sie gleichzeitig vollständig zu erhalten.

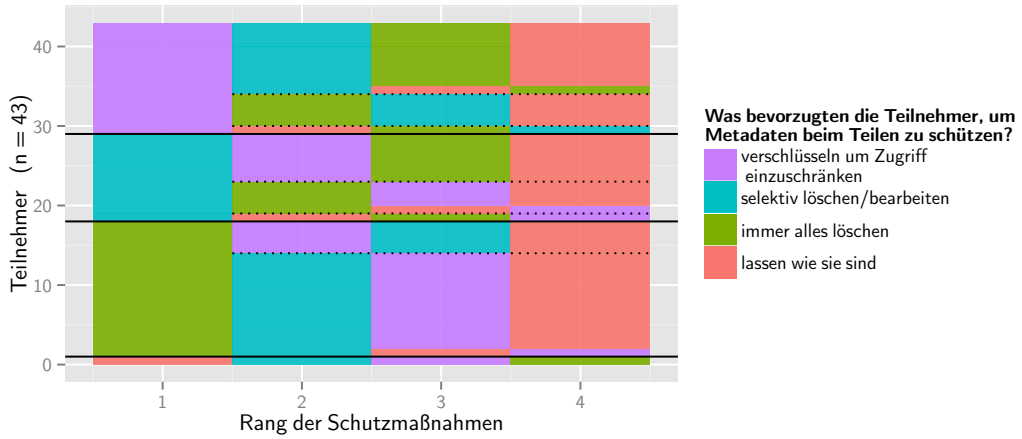


Abbildung 6.10: Bevorzugte Maßnahmen zum Schutz von Metadaten vor Fremdzugriffen

6.3.6 Abschluss und Zusammenfassung

Zum Abschluss der Laborstudie wurden die Teilnehmer gefragt, ob sie durch die Erprobung der neuen Browser-Funktionen etwas dazu gelernt oder wahrgenommen hätten, wodurch sich etwas an ihrer Meinung, ihrer Einstellung oder an ihrem Verhalten ändern könnte. 88 % der Teilnehmer bejahten diese Frage. Rund ein Viertel von ihnen gab ab, dass sie versuchen würden, mehr über Metadaten nachzudenken und anstreben, solche Informationen zukünftig vor dem Teilen zu modifizieren. Andere gaben an, dass sie sich nun weitaus mehr über Metadaten und die Problematik des verborgenen Teilens der Kontextinformationen bewusst sind, nachdem sie Realbeispiele gesehen haben. Dies zeigt deutlich, dass es ein klares Verlangen nach Veränderung gibt, sobald sich die Nutzer über das Vorhandensein von Metadaten

bewusst sind. Mehr als 10 % der Teilnehmer gab in den Abschlusskommentaren an, dass sie die Menge und Art der eingebetteten Metadaten unterschätzt hätten. Selbst Teilnehmer, die der Meinung waren zu wissen, was alles gespeichert werden kann, waren überrascht, als sie eingebettete Personen-Markierungen oder die eingebetteten Vorschaubilder entdeckten.

Bevor die Laborstudienteilnehmer darüber aufgeklärt werden konnten, dass die neuen Funktionen Teil einer selbst entwickelten Browser-Erweiterung waren und nicht Teil einer neuen Version des Browsers Chrome, fragte rund ein Viertel der Teilnehmer wann und wo sie den Browser mit den neuen Funktionen erhalten könnten. Selbst nachdem sie darüber informiert worden waren, dass es sich bei der Erweiterung um einen Prototyp handele, wollten einige von ihnen diesen direkt nutzen.

6.3.7 Fazit

Die Online-Umfrage zur Teilnehmer-Rekrutierung hatte gezeigt, dass rund 70 % der Teilnehmer ein vages Verständnis über die Existenz von Metadaten hat. Mehr als die Hälfte dieser gab an, kein Detailwissen über enthaltene Informationen zu besitzen, geschweige denn zu wissen, was die von ihnen verwendeten Webdienste mit den enthaltenen Informationen machen. Zu Beginn der Laborstudie gaben die Teilnehmer außerdem an, ein eher geringes Gefühl von Kontrolle zu besitzen, was sie von sich im Web preisgeben.

Die Laborstudie offenbarte eine sehr positive Reaktion der Teilnehmer darauf, dass sie sehen und kontrollieren können, was sie zusammen mit Fotos im Web teilen. Ebenso positiv begrüßten sie sehen zu können, welche verborgenen Informationen Bilder im Web enthalten. Die Evaluierung der Nutzbarkeit des Kontrollmechanismus beim Hochladen und der Visualisierungsfunktionen zeigte sehr gute Ergebnisse, so dass die Entwicklung und Evaluierung fortgeführt werden sollte. Das Ziel der weiteren Entwicklung sollte sein, die Methoden so weiter zu entwickeln, dass sie Bewusstsein in der Praxis schaffen können. Außerdem müssen praxistaugliche Werkzeuge geschaffen werden, die der Kontrolle und dem Schutz von Metadaten dienen, sobald bei den Nutzern der Wunsch nach Veränderung entstanden ist.

In der Laborstudie wurden die Nutzer informiert, was untersucht werden sollte, so dass vorwiegend nur die Nutzbarkeit der Implementierung evaluiert werden konnte. Eine explizite Evaluierung des Bewusstsein schaffenden Effekts und des aus der Nutzung resultierenden Wunsches nach Schutz der Metadaten muss folgen.

Der präsentierte Ansatz Metadaten auf Basis des CaaS-Paradigmas zu verschlüsseln, wurde in der Laborstudie ansatzweise durch eine Mock-up-Implementierung untersucht. Die Ergebnisse zum Einsatz von Verschlüsselung zeigten ein so nicht erwartetes hohes Interesse an der Verschlüsselung zum gleichzeitigen Erhalt und Schutz von Metadaten, so dass auch dieses noch genauer untersucht werden sollte.

6.4 Zusammenfassung

Metadaten können einen erheblichen Teil zur Bedrohung durch geteilte Fotos beitragen, weswegen sie heute oft schlichtweg gelöscht werden, wenn Bilder im Web geteilt werden. Mit dem Löschen der Metadaten werden jedoch auch nutzbringende Informationen gelöscht, die besonders den einzelnen Nutzer helfen können, die stetig steigende Menge an Bildern besser zu beherrschen. Auch die Teilnehmer der vorgestellten Studie gaben an, dass sie Metadaten als nützlich und sinnvoll ansehen. Sie gaben jedoch auch an, dass sie Metadaten außerhalb ihres Kontrollbereiches als Bedrohung wahrnehmen. Durch das Teilen von Fotos geben Nutzer teilweise die Kontrolle über die geteilten Bilder auf. Dies gilt ebenso für die in den Bildern enthaltenen Kontextinformationen, von denen viele Nutzer nicht wissen und deren Menge und Informationsfülle selbst zum Teil von denen unterschätzt werden, die meinen zu wissen, was gespeichert werden kann.

Um Metadaten zu nutzen, müssen diese erhalten werden. Sie müssen jedoch gegen den ungewollten Zugriff geschützt werden, um die Privatsphäre der Nutzer zu schützen. Bevor die Nutzer die Informationen jedoch schützen können, müssen sie sich über ihre Existenz und den Inhalt bewusst sein, um die Notwendigkeit des Schutzes zu erkennen. Die hier präsentierte Browser-Erweiterung adressiert diese Problematik und zeigt einen Ansatz wie Bewusstsein über Bild-Metadaten geschaffen werden kann. Sie tut dies sowohl für bereits geteilte Bilder als auch für Bilder, die Nutzer im Begriff sind zu teilen. Zusätzlich zeigt sie einen Ansatz wie die Preisgabe von Bild-Metadaten im Moment des Teilens eingeschränkt werden kann. Exemplarisch zeigt sie auch, wie Verschlüsselung als Schutzmaßnahme in den Prozess des Teilens und Betrachtens eingebunden werden kann. Die durchgeführte Laborstudie zeigte, dass die Ansätze der Browser-Erweiterung sehr positiv von den Nutzern begrüßt wurden, und dass die gewählte Implementierung von den Teilnehmern als gut nutzbar empfunden wurde. Zumindest im Rahmen der Laborstudie konnte das Bewusstsein über Bild-Metadaten durch die neuen Browser-Funktionen verbessert werden. Vor allem konnte auch ein Verlangen nach Schutz erzeugt werde. Im Kombination mit weiterzuentwickelnden Schutzmaßnahmen bilden die Schaffung von Bewusstsein und das resultierende Verlangen nach Schutz und Kontrolle die Grundlage für eine zukünftige informierte Nutzung und Erhaltung von Metadaten als realistische Alternative zum Vernichten der Kontextinformationen.

Kapitel 7

Standortbezogene Funktionen mobiler Geräte

Der aktuelle Aufenthaltsort eines Nutzers ist eine auf mobilen Geräten viel verwendete Kontextinformation. Aus diesem Grund sollte besonders auf diesen Geräten der Schutz der Standortinformationen ausreichend ermöglicht werden. Die Bedrohungsanalyse in Abschnitt 4.2 zeigte, welche Bedrohungen durch die Preisgabe der Informationen andernfalls entstehen könnten.

Insbesondere das mobile Betriebssystem Android war in der Vergangenheit häufig im Fokus von Betrachtungen der Privatsphäre, da für dieses neben vielen legitimen standortbezogenen Apps auch viele Apps existieren, bei denen der Standortzugriff aus Nutzersicht fragwürdig ist. Dies betrifft vor allem kostenfreie Apps, die Standortinformationen sammeln, um sie für integrierte In-App-Werbung zu verwenden, jedoch auch solche, bei denen der Grund für die geforderten Rechte nicht ersichtlich ist. Die Quelloffenheit des Systems machte Android zum Gegenstand diverser Forschungsarbeiten sowie verschiedener Community-Entwicklungsprojekte. Die im Folgenden beschriebenen Arbeiten konzentrieren sich auch auf dieses System. Die Konzepte lassen sich jedoch auf alle mobilen Betriebssysteme übertragen.

Standortnutzung von Android-Apps Um sich einen Eindruck zu verschaffen, wie viele Android-Apps den Zugriff auf Standortinformationen verlangen, wurde im Rahmen der hier beschriebenen Arbeiten die Web-Version von Googles App-Marktplatz, dem *Play Store*, analysiert. Zum Zeitpunkt der Erhebung im Juni 2013 waren über die Webseiten 20.681 beliebte Apps zu finden. 27,2 % dieser Apps benötigten für die Installation die Berechtigung zum Zugriff auf Standortinformationen eines Gerätes. Unterteilt man die Apps in kostenpflichtige und kostenfreie Apps, so verlangten 17 % der kommerziellen und 34 % der kostenlosen Apps die Berechtigung für den Zugriff auf genaue (GPS-) oder grobe (WLAN-) Standortinformationen.

Im Rahmen anderer Forschungsarbeiten wurden ebenfalls Informationen über die

geforderten Berechtigungen von Android-Apps erhoben: Zwischen Dezember 2013 und April 2014 wurden dabei 1,17 Millionen kostenlose Android-Apps (circa 98 % der kostenlosen Apps aus dem Play Store) erfasst und analysiert. Von all diesen Apps verlangten 29,7 % den Zugriff auf genaue Ortsinformationen und weitere 3,9 % den Zugriff auf ausschließlich grobe Standortinformationen.

Der Anteil an Apps, die Standortinformationen verlangen, ist hoch. Will ein Android-Nutzer eine dieser Apps nutzen, muss er ihr die Berechtigungen für den Standortzugriff geben. Will er den Zugriff im Weiteren vermeiden, bleibt ihm bei den meisten Android-Varianten bisher nur, die Standortdienste zeitweise zu deaktivieren. Viele Nutzer übersehen dabei jedoch, dass Apps im Hintergrund weiter laufen und Informationen erfassen können, wenn sie nicht aktiv beendet werden, sondern die Nutzer nur andere Apps öffnen oder zum Homescreen wechseln.

Faktor Standortgenauigkeit Will ein Nutzer standortbezogene Funktionen einer App verwenden, kann er seine Privatsphäre jedoch nicht durch das Deaktivieren schützen. In diesem Fall ist vielmehr der folgende Aspekt zu beachten: Werden einer App Standortinformationen zur Verfügung gestellt, so wird dies immer[1] mit der maximalen Genauigkeit getan. Dies gilt sowohl für Android als auch für Apple iOS. Karten-Apps, Apps zur Navigation, Apps zum Teilen des eigenen Standortes, Wettervorhersage-Apps oder auch Internetradio-Apps erhalten alle dieselben Informationen, unabhängig von den bereitstellten Funktionen und unabhängig davon, ob sie solch eine Genauigkeit benötigen.

Während einige Apps, wie beispielsweise die zur Navigation, die genauen Ortsangaben für die Erfüllung ihrer Aufgaben unumstritten benötigen, existiert eine Vielzahl von Apps, die vollständig korrekt oder mit nur geringen Einschränkungen mit weitaus gröberen Standortinformationen funktionieren würden. In solchen Fällen, wie beispielsweise bei der Standortangabe von Statusmeldungen in Sozialen Onlinenetzwerken, dem Erhalt lokaler Rabattcoupons oder der standortbezogenen In-App-Werbung kann die Privatsphäre der Nutzer geschützt werden, ohne die gewünschte Funktionalität einzuschränken, indem die Genauigkeit verringert wird.

Mit Ausnahme der Wahl der Standortquelle unter Android haben die Nutzer mobiler Geräte keine Möglichkeit die Genauigkeit der preisgegebenen Ortsinformationen zu beeinflussen. Und selbst Androids Einflussmöglichkeit bietet keinen Schutz der Privatsphäre, da die Ortsbestimmung durch die WLAN-basierte Ortung meist ausreichend genau ist, um eine Bedrohung verursachen zu können.

[1] Eine Ausnahme bildet Android hier: Eine App mit der ausschließlichen Berechtigung für den Zugriff auf grobe Ortsinformationen erhält veränderte Informationen, falls nur genaue Daten vorliegen: Die Koordinaten werden auf ein gröberes räumliches Raster abgebildet. Außerdem wird das erlaubte Abfrageintervall begrenzt. Dies betrifft jedoch nur einen geringen Teil der Apps.

Dieses Kapitel befasst sich im Weiteren damit, Nutzern bessere Einflussmöglichkeiten an die Hand zu geben. Es werden Lösungen vorgestellt, wie Nutzer die preisgegebenen Daten so einschränken können, dass sie möglichst wenig über ihren Standort preisgeben, während sie standortbezogene Dienste nutzen. Außerdem soll den Nutzern die Möglichkeit gegeben werden, besser über die Verwendung ihrer Kontextinformationen informiert zu sein, so dass sie fundierte Entscheidungen über die Nutzung von Apps fällen können.

7.1 Kritische Würdigung bisheriger Ansätze

In Abschnitt 3.3.2 wurden verschiedene Implementierungen und wissenschaftliche Arbeiten zum Schutz der Privatsphäre vorgestellt, die der Preisgabe von Standortinformationen begegnen. Soll jedoch nicht nur die Preisgabe des eigenen Standortes gegenüber Apps/Anbietern verhindert werden, sondern sollen mit einem Gerät auch standortbezogene Dienste verwendet werden, so besitzen die beschriebenen Schutzmaßnahmen deutliche Einschränkungen.

Reagiert ein verändertes System wie im Fall des Rechte-Widerrufs bei CyanogenMod 7 auf eine Standortanfrage mit einem (beabsichtigten) Ausnahmefehler, so müssen die anfragenden Apps mit diesem umgehen. Da die Apps solch einen Fehler eigentlich nicht erwarten müssen, existieren eventuell keine entsprechenden Fehlerroutinen, was zu Fehlverhalten bis hin zur sofortigen Beendigung führen kann. Solch eine Lösung ist als kritisch zu betrachten. Sie kann dafür verantwortlich sein, dass Nutzer App-Fehler erleben, wobei der Fehler nicht durch die App, sondern durch eine Manipulation des unterliegenden Systems entsteht.

Wird einer App durch den Rückgabewert `null` vorgegaukelt, dass keine Ortsinformationen vorhanden sind oder festgestellt werden können [76, MockDroid], so ist dies aus Sicht des Privatsphäreschutzes und für die Wahrung der Funktionsfähigkeit von Apps eine akzeptable Lösung. Mit diesem Rückgabewert muss jede App umgehen können und gleichzeitig verhindert dies eine Preisgabe von Informationen. Apps, deren Hauptfunktionen nicht auf Ortsinformationen beruhen, funktionieren eingeschränkt. Standortbezogene Dienste können jedoch nicht verwendet werden.

Gibt ein System einer App fixe Koordinaten zurück wie etwa den Standort des Google-Firmensitzes in Mountain View, Kalifornien [110, AppFence] oder die Null-Koordinaten im Golf von Guinea im Atlantischen Ozean [74, MyShield], so hilft dies dem Schutz der Privatsphäre vor Werbeanbietern, jedoch schlägt diese Lösung vollkommen fehl, wenn standortbezogene Dienste verwendet werden sollen. Für die Rückgabe zufälliger Koordinaten [51, PDroid 2.0] gelten dieselben Einschränkungen. In beiden Fällen werden Apps in dem Glauben gelassen, den aktuellen Standort zu erhalten, doch hat dieser keinen sinnvollen Bezug zum wahren Ort des Nutzers, so

dass standortbezogene Dienste nicht verwendet werden können.

Von allen vorherigen Publikationen bietet MyShield [74] solchen Apps, denen vom Nutzer eingeschränktes Vertrauen zugestanden wird, die beste Lösung, welche sowohl die Privatsphäre als auch die Funktionalität zu gleich wahrt. Durch das Abschneiden der Koordinatenwerte nach der ersten Nachkommastelle (Differenz $< 0{,}1°$) wird der genaue Ort einer Person nicht preisgegeben, jedoch bleibt ein Bezug zu ihrem wirklichen Ort. Somit ist zu erwarten, dass auch ein gewisser Teil der standortbezogenen Dienste hinreichend funktioniert. Das Abschneiden der geographischen Breite schafft eine Ungenauigkeit auf der Nord-Süd-Achse von bis zu grob 11 km. Das Abschneiden der geographischen Länge schafft abhängig von der Breite eine Ungenauigkeit auf der Ost-West-Achse von bis zu grob 11 km am Äquator und beispielsweise grob 6,8 km in der Region Hannover. Somit wird der Standort etwa in der Größenordnung einer Mittelstadt genau an die App gegeben. Eine Einschränkung dieser Methode bleibt, dass die Ungenauigkeit vom jeweiligen Ort des Nutzers abhängt: Wie groß der abgeschnittene Teilwert ist, und wie groß die daraus resultierende Ungenauigkeit ist, ist weder konstant noch ohne Weiteres für den Nutzer vorhersagbar.

Verlangt und verwendet eine Android-App nur grobe Ortsinformationen, so werden genaue Ortsangaben, wie die einer GPS-Ortung, durch den `LocationFudger` verändert. Die genaue Ortsangabe wird auf ein Gitter abgebildet, dessen Punkte mindestens 200 Meter und im Standardfall 2.000 Meter Abstand haben, nachdem die Koordinaten um einen zufälligen Wert verschoben wurden, welcher meist kleiner als der gegebene Gitterpunktabstand ist. Die Android-Nutzer wissen nicht, wann der `LocationFudger` verwendet wird. Auch kennen sie die verwendeten Parameter nicht. Die Veränderung des Ortes durch Android selbst findet nur für Apps statt, die von sich aus keine genauen Ortsangaben bekommen wollen. Die Kontrolle liegt in der Hand der Entwickler und nicht beim Nutzer. Dies ist eine sinnvolle Methode, um Daten aus genauen Standortquellen für Apps mit Berechtigungen für grobe Angaben zu verwenden. Es ist keine Schutzfunktion für die Privatsphäre der Nutzer.

7.2 Ein Framework zur Standortverschleierung für Android

In den vergangenen Jahren wurde eine Vielzahl von Methoden zur Verschleierung von Standortinformationen publiziert, die zum Ziel haben, die Privatsphäre der Nutzer zu schützen. Die meisten dieser Arbeiten waren jedoch eher von theoretischer Natur. Die Anwendbarkeit der Methoden im Kontext moderner mobiler Geräte wurde bis heute nicht evaluiert. Auch der Aspekt der Nutzbarkeit wurde in der Forschung nur selten beachtet. Die veröffentlichten Methoden reichen dabei von autarken Lösungen, die Koordinaten verschieben [72] und somit direkt auf einem Gerät imple-

mentiert werden könnten, bis hin zu webbasierten Lösungen, welche die Positionen anderer Nutzer berücksichtigen, um beispielsweise k-Anonymität herzustellen [99]. Um die verschiedenen Methoden zur Verschleierung auf den heutigen mobilen Geräten in der Praxis evaluieren zu können, wurde das *Standortprivatsphäre-Framework* für Android entwickelt [102].

7.2.1 Design und Implementierung

Das Standortprivatsphäre-Framework ermöglicht Entwicklern eine einfache Integration verschiedener Verschleierungsmethoden in das mobile Betriebssystem. Die implementierten Methoden stehen allen installierten Apps zur Verfügung, so dass diese selbst keine Verschleierung implementieren müssen. Nutzer des modifizierten Android-Systems können für jede App, die Standortinformationen verwendet, sowie für das Android-System selbst eine eigene Methode und Konfiguration festlegen. So können die Ortsinformationen für jede App individuell verschleiert werden.

Die Verschleierung kann von einem Nutzer zentral für alle Apps aktiviert oder deaktiviert werden. Erfragt eine App Standortinformationen, so werden diese mit einer globalen Standardmethode verschleiert, solange für eine App keine individuelle Konfiguration festgelegt worden ist. Die Verschleierung ist somit eine Opt-out-Funktion für alle neu installierten Apps. Der Nutzer kann im Verlauf die Verwendung der Verschleierung für eine App deaktivieren oder abweichend von der globalen Methode eine individuelle Verschleierung festlegen. Die Konfiguration geschieht dabei über die existierende App *Einstellungen*.

Das Standortprivatsphäre-Framework wurde ursprünglich auf Basis der Android-Distribution CyanogenMod 9.1 (Android 4.0.4 – *Ice Cream Sandwich*) implementiert und auf einem Smartphone vom Typ *Samsung Galaxy Nexus* erprobt [156]. Später wurde es auf CyanogenMod 10.1 (Android 4.2 – *Jelly Bean*) portiert und mit einem Smartphone vom Typ *LG Nexus 4* detailliert getestet.

Das Framework besteht aus drei verschiedenen Komponenten: ein Modell für Verschleierungsmethoden und Konfigurationen; die Kontrollkomponente, welche die konfigurierten Verschleierungsmethoden auf die wahren Standortinformationen anwendet; eine Erweiterung der Einstellungen-App, die den Nutzern die Konfiguration der Verschleierung ermöglicht. Die einzelnen Teile der Komponenten und ihre Integration in das Betriebssystem sind in Abbildung 7.1 dargestellt.

7.2.1.1 Modell

Das Modell definiert den `AbstractLocationPrivacyAlgorithm` als Vorlage für die Implementierung der Verschleierungsmethoden. Für jede Verschleierungsmethode müssen je zwei Methoden implementiert werden.

Die Methode `obfuscate()` dient der Verschleierung einer Standortinformation. Als Eingabeparameter erhält sie die wahre Standortangabe. Als Rückgabewert liefert sie den verschleierten Ort. Der bereitgestellte `Context` ermöglicht die Umsetzung komplexerer Methoden, die externe Funktionen verwenden, wie beispielsweise den Geocoder des Android-Systems oder einen Dienst im Web.

Die Methode `getDefaultConfiguration()` dient der Definition von Konfigurationsparametern und der Festlegung von Standardwerten der `LocationPrivacyConfiguration` einer Verschleierungsmethode. Wird eine Verschleierung neu für eine App gewählt, werden diese Werte als Grundeinstellung verwendet. Die Sichtbarkeit der verschiedenen Parameter in der Einstellungen-App wird ebenfalls im Modell festgelegt: Sie können sichtbar und vom Nutzer veränderbar sein, Eingaben wie Passwörter können maskiert werden und es können für den Nutzer nicht sichtbare Parameter definiert werden. Letztere dienen vorwiegend der Speicherung von Werten statusbehafteter Verschleierungsmethoden: Sie können beispielsweise den vorherigen wahren Standort speichern, um verschleierte Koordinaten nur zu aktualisieren, wenn sich der Nutzer um eine festgelegte Distanz bewegt hat. Der festgelegte Typ eines Konfigurationsparameters (wie Ganzzahl, Wahrheitswert, Koordinate) bestimmt automatisch die Visualisierung und die Nutzerschnittstelle zur Modifikation in den Einstellungen. Die Benennung und Beschreibungen einer Verschleierungsmethode und ihrer Parameter werden in Androids XML-basierten Sprachdefinitionen festgelegt.

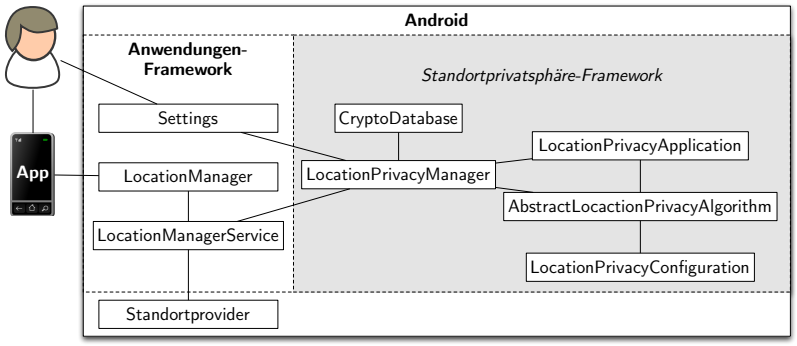


Abbildung 7.1: Komponenten und Integration des Standortprivatsphäre-Frameworks

7.2.1.2 Kontrollkomponente

Der `LocationPrivacyManager` ist die zentrale Komponente des Frameworks. Er stellt alle Funktionen zur Verwaltung des Frameworks und zur Verschleierung der Standortinformationen bereit. Die Konfiguration des Frameworks wird in der verschlüsselten `CryptoDatabase` gespeichert. Wird der `LocationPrivacyManager` nach dem Start des Systems erzeugt, so liest dieser den geheimen Schlüssel für die Datenbank aus seinen privaten `SharedPreferences`. Existiert dieser beim erstmaligen Starten nicht, werden ein zufälliger Schlüssel und die Datenbank neu erzeugt. Der `LocationPrivacy`

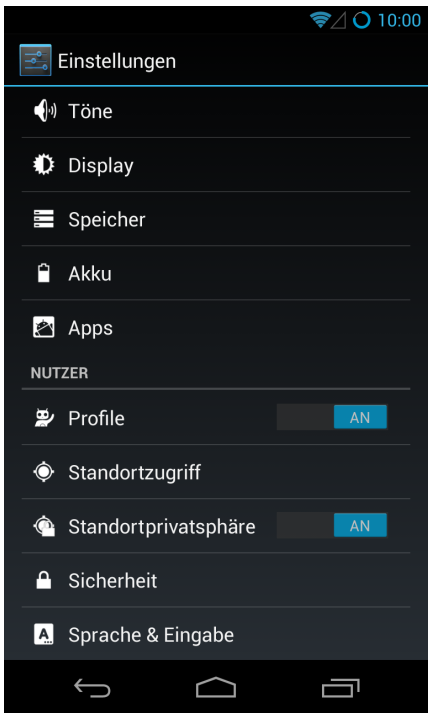
`Manager` verwaltet die Datenbank für die Speicherung der Konfigurationen und den Zugriff auf diese. Er hält die Konfigurationen im Speicher, um die Verschleierung zu beschleunigen. Wird eine Konfiguration durch den Nutzer geändert, so wird die Änderung in der Datenbank gespeichert. Über einen Broadcast wird der `LocationPrivacyManager` dazu veranlasst, die veränderte Konfiguration neu einzulesen.

Die Methode `obfuscateLocation()` implementiert die Verschleierung einer Standortinformation wie folgt: Wird sie mit dem Standort `null` (kein Ort bekannt) aufgerufen, so ist auch der verschleierte Ort `null`. Ist das Standortprivatsphäre-Framework deaktiviert, so wird der wahre Standort zurückgegeben. Andernfalls wird geprüft, ob eine Konfiguration im Cache liegt oder in der Datenbank vorhanden ist. Ist keine Konfiguration vorhanden, greift eine App erstmals auf Standortinformationen zu. In diesem Fall wird eine Konfiguration für die App angelegt, in der die globale Standardmethode als Verschleierungsmethode festgelegt ist. Nun, wo eine Konfiguration für die App vorhanden sein muss, wird geprüft, ob die Standortverschleierung für die betroffene App aktiviert ist. Ist dies der Fall, wird die Ortsinformation mit der konfigurierten Methode verschleiert.

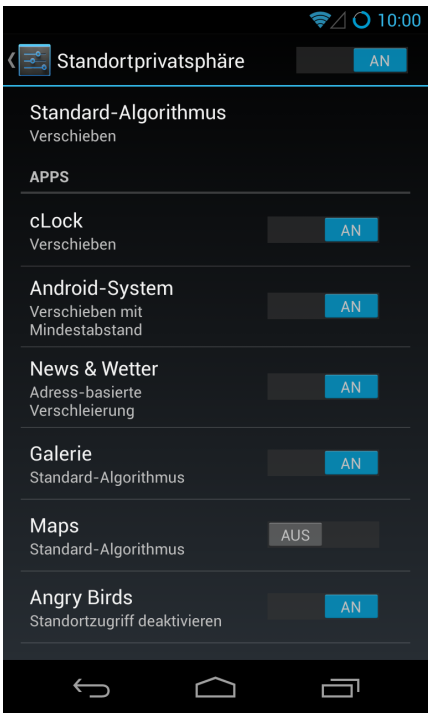
7.2.1.3 Einstellungen

Die Konfiguration der Standortverschleierung wurde, wie in Abbildung 7.2a dargestellt, in die Einstellungen-App integriert. Der in den Menüpunkt *Standortprivatsphäre* integrierte Schalter erlaubt zu sehen, ob das Framework aktiv ist. Gleichzeitig ermöglicht er das schnelle Aktivieren oder Deaktivieren. Über den Menüpunkt erreicht der Nutzer die Einstellungen des Frameworks. Die Hauptansicht der Standortprivatsphäre-Einstellungen gibt dem Nutzer einen schnellen Überblick über die konfigurierten Methoden. Wie in Abbildung 7.2b zu sehen ist, zeigt sie die gewählte globale Methode an sowie eine Liste aller Apps, die bisher auf Standortinformationen zugegriffen haben. Für jede dieser Apps werden die gewählte Methode und der Status der Verschleierung dargestellt.

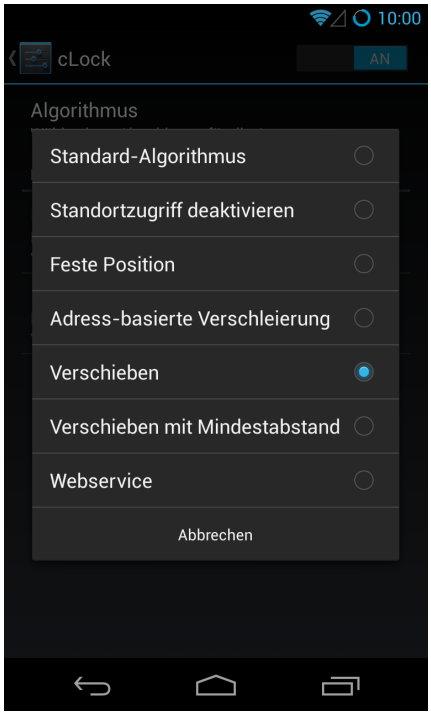
Durch die Auswahl einer App öffnen sich die Detaileinstellungen für diese. Ein Nutzer kann die zu verwendende Methode wie in Abbildung 7.2c dargestellt auswählen. Abhängig von der jeweiligen Methode werden die Konfigurationseinträge für die verschiedenen Parameter gemäß der Festlegungen im Modell angezeigt. Dem Typ eines Parameters entsprechend wird ein passendes Soft-Keyboard eingeblendet. Wahrheitswerte werden als Checkboxen dargestellt und Auswahllisten als Dropdown-Auswahlfeld. Passworte werden mit Sternchen maskiert. Verändert ein Nutzer einen Parameter vom Typ Koordinate, wird eine wie in Abbildung 7.2d dargestellte Kartenauswahl geöffnet: Der Nutzer kann einen Punkt auf der Karte wählen, nach einer Adresse suchen oder direkt Koordinaten im Suchfeld eingeben. Zu einem gewählten Punkt wird die ermittelte Adresse eingeblendet.



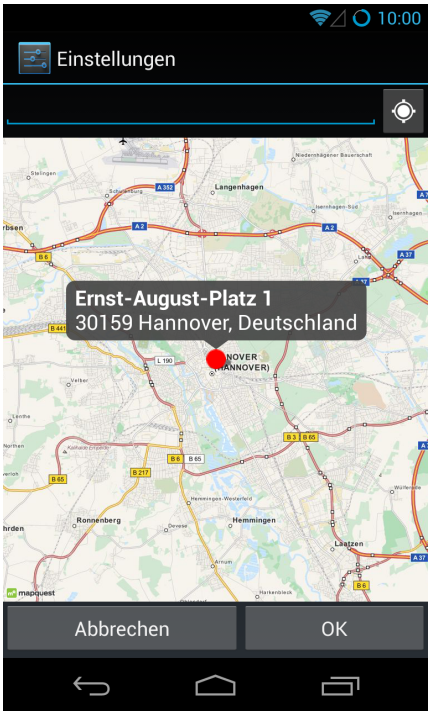
(a) Integration in Einstellungen



(b) App-Einstellungen



(c) Algorithmen-Auswahl



(d) Ortsauswahl auf Karte

Abbildung 7.2: Bildschirmfotos des Standortprivatsphäre-Frameworks

7.2.1.4 Integration des Frameworks

Eine Android-App kann auf den aktuellen Standort eines Gerätes zugreifen, wenn die App die Berechtigungen für den Zugriff auf die Informationen spezifiziert und bei der Installation erhalten hat und zusätzlich der Standortzugriff global aktiviert ist. Um auf die Standortinformationen zuzugreifen, erstellt eine App eine Instanz von Androids `LocationManager`. Jede dieser Instanzen erhält die Standortinformationen vom zentralen `LocationManagerService`, der im Betriebssystem-Kontext im Anwendungen-Framework läuft. Dieser erhält Standortdaten wiederum von den verschiedenen Standortprovidern aus den unterliegenden Betriebssystemschichten.

Abbildung 7.3 zeigt, über welche Mechanismen Apps Standortinformationen über den `LocationManager` beziehen können. Über die Methode `getLastKnownLocation()` kann eine App den letzten bekannten Standort des Gerätes abfragen. Um aktuelle Standortinformationen zu erhalten, kann die App einen `LocationListener` registrieren. Dieser meldet der App den aktuellen Standort des Gerätes, sobald dieser festgestellt werden kann, in Abhängigkeit von vorab festgelegten Aktualisierungsparametern, wie etwa der minimalen Distanz zweier Ortsangaben. Alternativ zu einem Listener kann ein `PendingIntent` registriert werden, um aktuelle Standortinformationen zu erhalten. Um standortbezogene Funktionen zu realisieren, kann eine App ebenfalls einen `ProximityAlert` für vorgegebene Koordinaten registrieren. Jede Standortanfrage über den `LocationManager` durchläuft eine der zwei Methoden `getLastKnownLocation()` oder `callLocationChangedLocked()` des `LocationManagerServices`. Innerhalb dieser zwei Methoden wurde daher das Standortprivatsphäre-Framework verankert, um sämtliche Standortinformationen zu verschleiern.

Der `LocationManagerService` läuft in einem eigenen Prozess separat von den Apps des Nutzers. Um eine App zu identifizieren, die eine Standortanfrage gestellt hat, wird über den `Binder` ihre Nutzer-ID (*uid*) ermittelt. Diese dient in allen Teilen des Frameworks zur Identifizierung der App. Die Nutzer-ID wird einer App vom Betriebssystem bei ihrer Installation statisch zugeteilt. Die App wird daraufhin immer unter dieser Identität ausgeführt. In seltenen Fällen kann die *uid* jedoch nicht eindeutig sein: Wenige Apps laufen im Android-System mit einer geteilten Nutzer-ID. In diesem Fall teilen sich die Apps eine Standortprivatsphäre-Konfiguration.[2]

Da der LocationManagerService und die Einstellungen-App beide im Kontext des Android-Systems laufen, können beide auf dieselben Daten im Speicher und in der Datenbank zugreifen. Es ist keine Interprozesskommunikation notwendig.

Ein Nutzer muss eine neu installierte App weder von Hand hinzufügen, noch wurden Androids Routinen zur Installation oder Deinstallation verändert. Die gewählte

[2]Diese Beschränkung wurde mit der Verwendung von CyanogenMod 10 aufgehoben, indem zusätzlich der Paketname einer App zur Identifizierung verwendet wird.

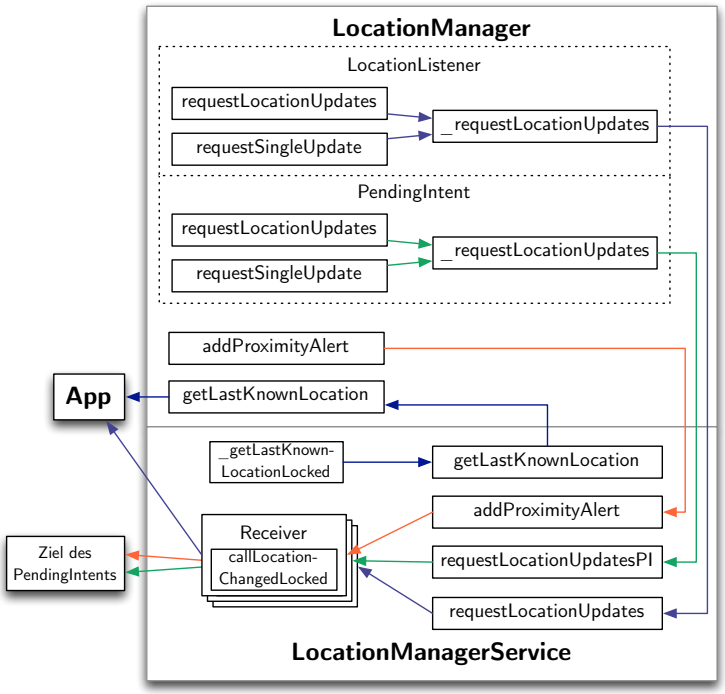


Abbildung 7.3: Fluss von Standortinformationen innerhalb von Android 4

Lösung erkennt automatisch, wenn eine bisher unbekannte App Standortinformationen abfragt. Sie erfasst neue Apps und versieht sie mit der globalen Standardverschleierung, da Methoden zum Privatsphäreschutz immer als Opt-out-Funktion umgesetzt werden sollten. Nutzer müssen sich bei der Installation einer App keine Gedanken über die Privatsphäre machen, die in diesem Fall ein klares Sekundärziel [150] ist. Benötigt eine App unveränderte Standortinformationen oder eine individuelle Verschleierung, können die Nutzer die Einstellungen für die App anpassen. Wird eine App vom System entfernt, so wird dies vom Standortprivatsphäre-Framework registriert und die entsprechende Konfiguration wird entfernt.

7.2.2 Verschleierungsmethoden

Im Rahmen der Implementierung des Standortprivatsphäre-Frameworks wurden die folgenden Verschleierungsmethoden exemplarisch implementiert.

7.2.2.1 Lokale Verschleierungsmethoden

Die lokalen Verschleierungsmethoden benötigen keinen Zugriff auf einen Dienst im Internet. Sie funktionieren auch, wenn keine Internetverbindung besteht. Die Methoden sind eher einfach gehalten, jedoch können sie in vielerlei Fällen ausreichend sein. Ihr Vorteil ist, dass der wahre Standort mit niemand anderem geteilt wird.

Deaktivierung Diese Methode implementiert eine Deaktivierung des Standortzugriffs je App, wie sie Apple iOS seinen Nutzern ab Version 6 aufwärts bietet. Anstatt einer Ortsangabe erhält eine App den Wert `null`. Diese geht folglich davon aus, dass kein Ort ermittelt werden konnte.

Feste Position Diese Methode erlaubt einem Nutzer die Festlegung fixer Koordinaten, die einer App bei jeder Standortanfrage zurückgegeben werden.

Verschieben Das zufällige Verschieben mit einer Maximalentfernung ermittelt zufällige Koordinaten innerhalb eines Kreises mit festgelegtem Radius, der um den wahren Ort des Nutzers gelegt wird [72]. Der Nutzer legt in der Konfiguration den Radius des Kreises fest. Außerdem spezifiziert er eine Distanz, um die sich der wahre Ort mindestens verändern muss, bevor die verschleierte Koordinate aktualisiert wird. Letzteres verhindert, dass sich die zufälligen Koordinaten bei jeder Anfrage ändern und so durch häufige Anfragen eine Art Streudiagramm verschleierter Orte entsteht, an dem man den wahren Ort des Nutzers nur ablesen braucht. Außerdem verhindert dieser Mechanismus, dass die Koordinaten häufig hin und her springen, was die Nutzbarkeit der Standortinformationen einschränken könnte.

Verschieben mit Mindestabstand Das zufällige Verschieben mit einer Maximalentfernung und einer Mindestdistanz erweitert die vorherige Methode. Bei dieser gibt ein Nutzer zusätzlich eine Mindestdistanz an, die der zufällige Ort vom wahren Ort entfernt sein muss. Dies verhindert, dass der zufällige Ort auf den wahren Ort fällt, auch wenn dies nur mit sehr geringer Wahrscheinlichkeit passieren könnte.

7.2.2.2 Dienstbasierte Verschleierungsmethoden

Die dienstbasierten Verschleierungsmethoden verwenden externe Dienste und benötigen daher eine funktionierende Internetverbindung. Die meisten standortbezogenen Apps benötigen diese jedoch auch. Aufgrund der Verzögerungen der Netzwerkkommunikation sind die dienstbasierten Methoden langsamer als vergleichbar komplexe lokale Methoden. Sie ermöglichen jedoch die Umsetzung komplexerer Verschleierungsverfahren, die beispielsweise auf externe Daten wie die Orte anderer Nutzer zurückgreifen. Bei der Verwendung einer solchen Methode gibt der Nutzer seinen wahren Ort gegenüber einem Privatsphäre-Dienst preis, während er ihn vor den Apps verbirgt. Prominente Beispiele sind Methoden die k-Anonymität herstellen.

Webservice Die Verwendung des generischen Webservice-Adapters ermöglicht die Nutzung eines externen Privatsphäre-Dienstes. Dieser ist über eine verschlüsselte HTTPS-Verbindung zu erreichen. Nutzer werden via Nutzername und Passwort authentifiziert. Soll eine Koordinate verschleiert werden, wird der Webservice mit den

wahren Koordinaten aufgerufen. Die Antwort enthält die verschleierte Ortsangabe, die an die anfragende App weitergegeben wird.

Adressbasierte Verschleierung Durch eine Kombination von Adresskodierung und Geokodierung wird der wahre Ort eines Nutzers auf die Koordinaten eines Geoobjektes abgebildet. Zur Verschleierung werden die wahren Koordinaten durch Adresskodierung in eine Postadresse überführt. Diese besteht aus verschiedenen Informationen wie Straße, Stadtteil, Stadt, Region und Land. Basierend auf der Einstellung des Nutzers werden Teile der Adresse – beispielsweise alle Informationen, die detaillierter als die Stadt sind – entfernt, um die Genauigkeit der Adresse zu verringern. Diese wird daraufhin durch Geokodierung zurück in Koordinaten überführt, die an die anfragende App weitergegeben werden. Auf diese Weise wird der Standort des Nutzers auf das nächstgelegene Geoobjekt vom gewählten Detailgrad – wie Stadt – abgebildet. Wie die Position des Objektes bestimmt wird, ist abhängig von der Geokodierung. Meist gibt sie die Mitte des umschließenden Rechtecks zurück. Ein Nachteil dieser Methode ist, dass sie von der Qualität der den Kodierungen zugrunde liegenden Geodaten abhängig ist. Die heute verfügbaren teils freien Geodienste, wie beispielsweise *Nominatim*/*OpenStreetMap* oder die Geodienste von Google, sind jedoch ausreichend für diesen Anwendungsfall. Ein positiver Aspekt der Methode ist, dass sie für viele Nutzer leicht zu verstehen ist, da keine technischen Parameter festgelegt werden müssen, sondern nur der Detailgrad, mit dem sie Aussagen treffen, wie „Ich bin in dieser Straße“ oder „Ich bin in dieser Stadt“. Die Implementierung umfasst die Detailgrade Straße, Postleitzahlenbereich, Stadt und Land. Für die Kodierung wird Androids integrierte Geocoder-API verwendet, die auf den Diensten von Google Maps basiert. Pro Verschleierung sind zwei API-Aufrufe notwendig: Adresskodierung und Geokodierung. Zur Steigerung der Performanz könnte die vollständige Implementierung in einen unabhängigen externen Dienst ausgelagert werden, der beispielsweise die Geodaten des OpenStreetMap-Projektes verwendet. Dies würde die Verzögerung durch Netzwerkkommunikation halbieren und die Nutzer müssten nicht auf einen Dienst von Google vertrauen.

7.2.3 Evaluierung des Frameworks

Das Standortprivatsphäre-Framework wurde einer grundlegenden Evaluierung unterzogen, die im Folgenden beschrieben wird.

7.2.3.1 Performanz

Die Verwendung des Frameworks sollte keinen merklichen, störenden Einfluss auf die Performanz des Gesamtsystems ausüben. Um dies zu testen, wurden mit einer Test-App vielfache Anfragen an die Methode `getLastKnownLocation()` gestellt und die

verbrauchte Zeit gemessen. Bei der Verwendung dieser Methode zur Standortabfrage wird keine Zeit durch die Ortung eines Standortproviders verbraucht, da nur der gepufferte Standort abgefragt wird, der jedoch jedes Mal erneut verschleiert wird. Die Messungen wurden auf einem frisch installierten Samsung Galaxy Nexus mit Dual-Core Cortex-A9-ARM-Prozessor und 1 GB Hauptspeicher durchgeführt.

Es wurden Zeitmessungen für vier verschiedene Konfigurationen gemacht. CyanogenMod 9.1 ohne das Standortprivatsphäre-Framework; das erweiterte System mit deaktiviertem Framework; das erweiterte System mit aktiviertem Framework und deaktivierter Verschleierung für die Test-App; das erweiterte System mit aktiviertem Framework und aktivierter Verschleierung für die Test-App. Für jede Konfiguration wurden mehrfache Durchläufe mit jeweils 10.000 Standortanfragen durchgeführt. Für die Verschleierung wurde die lokale Methode *Verschieben* verwendet. Es konnte keine merkliche Verzögerung durch das Framework gemessen werden. Unabhängig von der Test-Konfiguration benötigte jeder Durchlauf insgesamt zwischen 4,2 und 4,9 Sekunden. Daraus lässt sich schließen, dass das Framework selbst keinen messbaren negativen Einfluss auf die Performanz des Systems ausübt.

Die implementierten Methoden wurden ebenfalls miteinander verglichen. Das Testgerät war hierzu über einen WLAN-Access-Point der Universität mit dem Internet verbunden. Ein Test-Webservice, der lediglich die Vorzeichen der Koordinatenwerte änderte, wurde im lokalen Netzwerk platziert. Tabelle 7.1 zeigt die Ergebnisse der Testläufe. Das deutliche Maximum der lokalen Methoden wurde durch die Änderung der Verschleierungsmethode provoziert: Nach dem Wechsel der Methode wird die neue Konfiguration aus der Datenbank geladen, sobald die nächste Verschleierung durchgeführt wird. Dies wurde im Fall des Maximums mitgemessen. Die durchschnittliche Verzögerung der lokalen Methoden kann als gleich angesehen werden. Der mit diesen verbundene Rechenaufwand ist ähnlich gering. Die hohe Dauer der adressbasierten Verschleierung ist mit der Verzögerung durch den zweimaligen Aufruf der Geocoder-API zu begründen. Ein einmaliger Aufruf des Webdienstes im lokalen Netz sorgte für eine geringfügig niedrigere Verzögerung. Zusammenfassend lässt sich feststellen, dass der gemessene Zeitverbrauch aller Methoden akzeptabel ist. Werden Standortanfragen im Hintergrund ausgeführt, sollte auch eine Verzögerung von bis zu einer Sekunde kaum merklich oder hinderlich sein.

Verschleierungsmethode	Zeitverbrauch [Sekunden]		
	Minimum	Mittelwert	Maximum
fixer Standort	0,0008	0,0012	0,0019
zufälliger Ort (max)	0,001	0,0013	0,005
zufälliger Ort (min/max)	0,001	0,0015	0,005
Webdienst	0,2	0,23	0,4
adressbasiert	0,2	0,46	1,0

Tabelle 7.1: Zeitverbrauch verschleierter Standortanfragen

7.2.3.2 Bedrohungsanalyse

Das Standortprivatsphäre-Framework läuft im Kontext des Android-Systems. Unprivilegierte Apps können somit weder auf den Speicher des Frameworks zugreifen, noch können sie den Inhalt der Konfigurationsdatenbank manipulieren, da diese verschlüsselt im Dateisystem gespeichert ist und der dazugehörige Schlüssel im geschützten Bereich des System-Kontextes gespeichert ist. Die Apps können weder die vom Nutzer festgelegte Konfiguration der Verschleierung ändern noch diese deaktivieren. Nur Apps mit Root-Rechten könnten die Verschleierung manipulieren.

Das Framework wurde entwickelt, um auf einfache Weise verschiedene Verschleierungsmethoden in Android integrieren zu können. Neben einer Evaluierung der technischen Umsetzung solcher Methoden war der Fokus des Schutzes darauf gerichtet, Nutzern zu ermöglichen, standortbezogene Apps zu verwenden, ohne ihren genauen Standort preisgeben zu müssen. Diese Ziele werden mit der beschriebenen Implementierung erreicht. Das Framework schützt Nutzer hingegen nicht gegen eine böswillige Überwachung ihrer Bewegung. Anstatt Standortinformationen abzufragen, die Android bestimmt, können solche Angreifer den Ort eines Opfers auch auf andere Weise überwachen. Sie können beispielsweise den Ort anhand der IP-Adresse des Gerätes grob bestimmen. Außerdem kann eine App mit entsprechenden Berechtigungen selbst auf Basis sichtbarer Mobilfunkmasten und WLAN-Access-Points unter Verwendung einer entsprechenden Datenbank den Ort eines Opfers bestimmen. Aus diesem Grund müssen böswillige Apps weiterhin von App-Marktplätzen entfernt werden. Ein nicht böswilliges Beispiel dieser alternativen Ortung, die somit zum Teil auch das Privatsphäre-Framework umging, wurde bei der Evaluierung des Framework gefunden: Die Ortsbestimmung der App *Google Maps* setzt unter bestimmten Bedingungen nicht allein auf die Funktionen des Betriebssystems.

Es ist vorstellbar, dass das Standortprivatsphäre-Framework missbraucht werden könnte, indem ein Nutzer gegenüber einer App oder einem Dienst vorgibt, anderswo zu sein, als er wirklich ist. Dies ist mit der gegebenen Implementierung möglich, jedoch gibt es längst verschiedene Apps auf den App-Marktplätzen, die dies ermöglichen. Somit birgt das Framework keine Möglichkeit für neue böswillige Aktionen.

7.2.3.3 Einschränkungen

Während der Tests diverser Apps traten keine merklichen Einschränkungen der Funktionalität auf und die Verschleierung funktionierte wie erwartet. Unter anderem wurden die Apps *Kamera*, *GPS Status*, *Locus Map*, *Foursquare*, *Yelp*, *Chrome*, der Standardbrowser von CyanogenMod sowie die auf JavaScript basierte Ortung innerhalb der Webbrowser getestet. Als einzige Ausnahme zeigte die App *Google Maps*, sowie die dazugehörige App *Local*, ein reproduzierbares unerwartetes Verhalten bei der Verwendung der Standortverschleierung. War der GPS-Empfänger des Testgerä-

tes aktiviert und wurde eine GPS-basierte Ortung durchgeführt, zeigte die App wie erwartet einen verschleierten Ort an. War jedoch GPS deaktiviert oder konnte der Ort nicht über GPS bestimmt werden, so zeigte die Maps-App überraschenderweise die wahre Position des Gerätes an. In diesem Fall schien die App selbst den Ort des Gerätes basierend auf umliegenden WLAN-Access-Points oder Mobilfunkmasten zu ermitteln, anstatt die entsprechenden groben Standortinformationen des Android-Systems zu verwenden. Eine andere Erklärung wäre, dass die App selbst direkt auf die vorhandenen Standortprovider zugreift und so Androids Standortdienst umgeht. Ein Aufruf der Methode `getLastKnownLocation()` nach der Verwendung von Maps auf einem neu gestarteten Gerät zeigte, dass keine Standortinformationen im Zwischenspeicher vorhanden waren. Dies lässt darauf schließen, dass der Standortdienst bis dahin keinen Standort ermittelt hatte. Tests mit anderen Apps zeigten hingegen die verschleierten groben Ortsangaben. Mit einem HTTPS-Proxy wurde der Datenverkehr der Maps-App analysiert und es wurden Aufrufe eines Dienstes unter `google.com/glm/mmap` gefunden. Über diese Webadresse wird auch ein webbasierter Ortungsdienst von Goole erreicht. In den beobachteten Nachrichten waren der Name des aktuell verbundenen WLANs und die MAC-Adresse des dazugehörigen Access-Points enthalten. Keine der zwei genannten Vermutungen über die alternative Ortsbestimmung konnte vollständig nachgewiesen werden, da die teils binären Nachrichten auch der Kartierung von Access-Points zugeschrieben werden können.

Unabhängig von der Methode, wie Google Maps bei fehlender GPS-Ortung den Ort eines Gerätes bestimmt, muss festgestellt werden, dass jedes Mal, wenn eine App eigene Methoden zur Ortsbestimmung implementiert, die Kernfunktionalität des Betriebssystems und damit das Standortprivatsphäre-Framework umgangen wird. Dies ist ein generelles Problem, welches nur vermieden werden könnte, wenn das Betriebssystem den Zugriff auf alle Informationen, die zur genaueren Ortung verwendet werden können, stärker einschränkt. Die Tests der übrigen Apps zeigten, dass diese die Funktionen des Betriebssystems verwendeten und somit das Ziel, die Privatsphäre der Nutzer im Rahmen standortbezogener Dienste zu schützen, erreicht blieb.

7.2.3.4 Nutzbarkeit

Das Standortprivatsphäre-Framework wurde entwickelt, um Verschleierungsmethoden auf mobilen Geräten testen zu können. Technisch versierte Nutzer können das Framework jedoch auch, so wie es ist, in der Praxis verwenden, um ihre Privatsphäre zu schützen. Durch die Vorgabe angemessener Standardparameter könnte das Framework wohl auch von einem Teil der weniger versierten Nutzern verwendet werden. Für das Anpassen von Parametern bleibt jedoch Wissen zu Standortinformationen und den eingesetzten Verschleierungsmethoden eine notwendige Voraussetzung.

7.2.4 Nutzbarkeit von Standortverschleierung

Damit eine Standortverschleierung für alle Nutzer in der Praxis realisiert werden kann, muss sich die Forschung verstärkt der Nutzbarkeit der Methoden widmen. Die Herausforderung liegt darin, dass die meisten Verschleierungsmethoden für Laien schon allein konzeptionell schwer zu verstehen sind, ganz davon abgesehen, dass irgendjemand ihre diversen Parameter konfigurieren muss. Verlangt man von den Nutzern, die Parameter gemäß ihrer eigenen Privatsphäre-Anforderungen festzulegen, so können dies wahrscheinlich viele nicht tun, da die Parameter ebenso schwierig wie die Konzepte zu verstehen sind. Nimmt man zum Beispiel das Konzept der k-Anonymität, so ist für die meisten Nutzer sicherlich nachvollziehbar, was es bedeutet nicht von $k-1$ anderen Personen unterschieden werden zu können. Für Nutzer, die jedoch eher in Abständen/Metern denken, ist es nahezu unmöglich zu wissen, was dies für die Genauigkeit der Angabe ihres Standortes im Einzelfall bedeutet. Welche Auswirkungen es beispielsweise darüber hinaus hat, ob sich ein Nutzer in einer Großstadt befindet oder irgendwo auf dem schwach besiedelten Land, wird vielen nicht klar sein. Selbst wenn bei einem Teil der Nutzer dieses Verständnis vorhanden wäre, bleibt es schwer, ein persönliches k zu wählen, das den eigenen Anforderungen genügt. Verständnisschwierigkeiten sind jedoch nicht auf komplexere Methoden beschränkt: So ist es auch nicht einfach zu beurteilen, welchen Gewinn es jeweils für die Privatsphäre hat, wenn der wahre Standort um 100 Meter oder 500 Meter verschoben wird. Diese Beispiele zeigen, dass die Nutzbarkeit der Methoden häufig schon mit der Greifbarkeit des zugrunde liegenden Konzepts steht oder fällt.

Die Nutzbarkeit von Verschleierungsmethoden wurde bisher von kaum einer wissenschaftlichen Arbeit genauer untersucht. Auch das beschriebene Framework adressiert dieses Thema nicht. Es kann jedoch dazu verwendet werden, verschiedene Methoden und das Verständnis der Nutzer in der Praxis zu evaluieren. Eine Evaluation der Methoden im Feld erlaubt, Realweltprobleme zu identifizieren, die beim Entwurf der technischen Verfahren nicht bedacht oder übersehen wurden. Die Evaluierung der Nutzbarkeit einer Methode kann eventuell jedoch auch zeigen, dass eine Methode nicht zu vereinfachen und eventuell praxisuntauglich ist. Besonders dies sollte jedoch im Sinne nutzbarer Methoden respektiert werden.

Neben der Evaluierung der Methoden, die Schutz bieten sollen, stellt sich außerdem die Frage, in welcher Form die Nutzer am Schutz ihrer Standortinformationen interessiert sind. Auch wenn sie nach Schutz verlangen, verlangen sie eventuell nicht nach dem bestmöglichen, sondern nur nach einem ausreichenden Schutz, den sie dafür selbst auch verstehen können. Auch dies ist ein wichtiger Aspekt für die Wahl passender Methoden.

Aus all diesen Überlegungen folgen verschiedene Anforderungen an eine nutzerfreundliche Standortverschleierung:

- Die den Nutzern gebotenen Verschleierungsmethoden müssen sorgfältig gewählt werden, so dass auch die Wünsche und Ziele der Nutzer durch die Auswahl berücksichtigt werden.
- Die ausgewählten Methoden müssen für die Nutzer deutlich erkennbare Unterschiede in Bezug auf die Konzepte, die Wirkung der Parameter und die erreichten Schutzziele der Verschleierung vorweisen. Die Nutzer sollten die Unterschiede verstehen können, um eine fundierte Wahl treffen zu können. Im Zweifelsfall heißt dies auch, sich auf eine Methode zu beschränken.
- Schwer greifbare Konzepte müssen möglichst leicht verständlich für den Nutzer dargestellt werden. Beispielsweise sollte die Abfrage purer Zahlen, wo es geht, durch alternative Darstellungen ersetzt werden. Eine Möglichkeit dafür wären eventuell Metaphern: Statt eine Zahl einzugeben, kann ein Nutzer beispielsweise festlegen, dass sein Standort zufällig „auf der Fläche eines Fußballfeldes“ gewählt werden soll. Statt im Fall von k-Anonymität ein k festlegen zu müssen, könnte ein Nutzer festlegen, so anonym sein zu wollen, „wie er es in einem Einkaufszentrum wäre“ [153]. Ebenso kann es helfen, Zahlen soweit möglich zu visualisieren. Ist dies nicht möglich, ist eine Alternative, sich auf solche Methoden zu konzentrieren, die von sich aus einfach zu verstehen sind. Die zuvor beschriebene adressbasierte Verschleierung beschränkt sich beispielsweise auf allgemein bekannte Konzepte wie Straße oder Stadt.
- Standardeinstellungen sollten so gewählt werden, dass die Privatsphäre eines Nutzers auch ausreichend geschützt ist, wenn er diese nicht verändert.
- Die auf mobilen Geräten eingesetzten Verschleierungsmethoden müssen in Echtzeit verschleiern können. Die Ortung und Verwendung von Standortinformationen findet bei vielen Apps im Rahmen aktiver Nutzerinteraktion statt, so dass keine merklichen Verzögerungen entstehen dürfen. Diese könnten andernfalls die Nutzer zur Deaktivierung der Schutzfunktion verleiten.

7.2.5 Fazit

Das Standortprivatsphäre-Framework erfüllt zwei Aufgaben: Es ermöglicht eine einfache Integration verschiedener Verschleierungsmethoden in das mobile Betriebssystem Android. Auf diese Weise ist es Entwicklern möglich, die Methoden im Kontext moderner mobiler Geräte zu evaluieren. Als erste Implementierung von Standortverschleierung für Android kann das Framework technisch versierte Nutzer dabei unterstützen, ihre Privatsphäre besser zu schützen. Während andere Arbeiten vorwiegend zum Ziel haben, die Preisgabe von Standortinformationen zu erkennen und zu verhindern, ermöglicht das Standortprivatsphäre-Framework eine privatsphärebewusste Nutzung standortbezogener Dienste: Nutzer können für jede App eine

eigene Standortverschleierung festlegen und so die Preisgabe manchen Apps gegenüber verhindern und anderen nur den Grad an Details zur Verfügung stellen, die für die Nutzung der gebotenen Funktionen notwendig sind. So können sie beispielsweise Spielen ohne Standortbezug den Zugriff auf die Informationen verwehren, einem Wetterdienst nur die Stadt, in der sie sich aktuell befinden, verraten und ihre Navigations-App gleichzeitig uneingeschränkt nutzen.

7.3 Eine nutzerfreundliche Umsetzung von Standortverschleierung für Android

Betrachtet man die vorherigen Ausführungen zur Nutzbarkeit, so liegt es recht nahe, dass ein Grund, wieso Standortverschleierung bis heute von den mobilen Betriebssystemen nicht adaptiert worden ist, die Komplexität der Verschleierungsmethoden ist, welche zuerst von den Nutzern verstanden werden müssen, um sie danach bewusst konfigurieren und verwenden zu können.

Für einen optimalen Schutz der Privatsphäre muss die Verschleierung von Ortsangaben einerseits von Anwendungsfall zu Anwendungsfall so gewählt werden können, dass die Funktionalität einer Anwendung nicht übermäßig eingeschränkt wird. Andererseits muss die gewählte Verschleierung auch einem für den Nutzer angemessenen Kompromiss zwischen Privatsphäre und nutzbarer Funktionen genügen. Der Schutz von Standortinformationen sollte unbedingt auf den Geräten der Nutzer umgesetzt werden, da es für die Wahrung der Privatsphäre das Beste ist, den Informationsgehalt von Daten vor ihrer Preisgabe soweit wie möglich zu beschränken, so dass Dienstanbietern gegenüber nicht unnötig viele Details preisgegeben werden. Auch für Anwendungsfälle in denen Informationen mit anderen Personen geteilt werden, ist es vorzuziehen die Daten des Nutzers von vornherein zu beschränken, anstatt sie später durch Zugriffsschutzmechanismen gegen unerlaubten Zugriff zu schützen.

Um diesem Ziel näher zu kommen, wurde aufbauend auf dem zuvor beschriebenen Framework eine nutzerfreundliche Umsetzung von Standortverschleierung für Android entworfen und implementiert [101]. Das Konzept basiert dabei auf den Ergebnissen einer qualitativen Erhebung von Nutzerbedürfnissen durch Fokusgruppen.

7.3.1 Fokusgruppen zur Nutzung und zum Schutz von Standortinformationen

Vorherige Nutzerstudien haben gezeigt, dass Nutzer daran interessiert sind, den Zugriff auf Standortinformationen [95] und die Genauigkeit der verwendeten Informationen [80, 141] zu beschränken. Während diese gezeigt haben, dass die Nutzer das Bestreben haben, das Detail preisgegebener Standortinformationen zu beschränken, wurde nicht genauer untersucht, in welcher Form dies effektiv und nutzerfreundlich

umgesetzt werden kann. Um genauer zu erfassen, welche Bedürfnisse Nutzer in der Praxis wirklich in Bezug auf Standortprivatsphäre haben, wurden Gruppendiskussionen in Form von Fokusgruppen durchgeführt. Diese Methode ermöglichte es, die Erfahrungen, die Anforderungen, die Sorgen und die Wünsche der Nutzer in Bezug auf die Privatsphäre von Standortinformationen genauer zu ergründen.

7.3.1.1 Durchführung und Demographie

Um Teilnehmer für die Fokusgruppen zu rekrutieren, wurden 1.510 Abonnenten des E-Mail-Verteilers für Studien und Umfragen zu Forschungsthemen der Arbeitsgruppe Distributed Computing & Security angeschrieben. Eingeladen wurde zu Gruppendiskussionen zur „alltäglichen Nutzung von Apps auf mobilen Geräten“. Im Laufe der Gruppendiskussionen wurde das Thema dann auf standortbezogene Apps gelenkt und schließlich auf den Aspekt der Privatsphäre. Auf diese Weise sollte einer Beeinflussung durch eine frühzeitige Erwähnung des Begriffs Privatsphäre vorgebeugt werden. Auf die Einladung hin beantworteten 98 Personen den Online-Fragebogen, welcher der Studienorganisation diente. In diesem Fragebogen wurden zudem demographische Angaben, die technische Expertise der Teilnehmer, ihre Erfahrung mit mobilen Geräten und ihre Erfahrung mit verschiedenen Arten von Apps erfasst. Außerdem wurden die Fragen für eine Privacy Segmentation nach Westin gestellt. Basierend auf den Antworten der Teilnehmer wurden drei möglichst ausgeglichene Gruppen mit insgesamt 19 Teilnehmern gebildet: 11 weibliche und 8 männliche Teilnehmer mit einem Durchschnittsalter von 24 ± 4 Jahren. Die Teilnehmer waren Studierende 14 verschiedener Studienrichtungen wie Jura und Maschinenbau. Von den Teilnehmern waren 12 Android-Nutzer und 7 iOS-Nutzer. Die selbst eingeschätzte technische Expertise der Gruppenmitglieder war leicht überdurchschnittlich im Vergleich zu den 98 ursprünglichen Rückmeldungen. Gemäß der Klassifikation nach Westin waren 9 Teilnehmer Privatsphäre-Fundamentalisten und 10 von ihnen waren Privatsphäre-Pragmatisten. Die Gruppendiskussionen wurden an drei verschiedenen Tagen innerhalb einer Woche durchgeführt. Jede Diskussion dauerte circa 90 Minuten. Jeder Teilnehmer erhielt eine Aufwandsentschädigung von 20 Euro. Weitere Informationen zur Teilnehmer-Rekrutierung und zu den Teilnehmern der Fokusgruppen sind in Anhang C.4 zu finden.

7.3.1.2 Nutzung standortbezogener Apps

Die meisten Teilnehmer gaben im Online-Fragebogen an, wöchentlich bis täglich verschiedene Apps zu nutzen, welche häufig auch Standortinformationen verwenden. Zu diesen gehörten unter anderem Apps für Fahrplanauskünfte öffentlicher Verkehrsmittel oder für Staumeldungen, Apps zur Navigation, Karten-Apps und Apps zur Wettervorhersage. Die meisten von ihnen gaben an, Inhalte bei Sozialen Online-

netzwerken zu teilen. Im Gegensatz dazu gaben nur sechs der 19 Teilnehmer an, gelegentlich ihren Standort mit anderen zu teilen.

Während der Fokusgruppen-Diskussionen gaben die meisten Teilnehmer an, ausgewählte standortbezogene Funktionen einiger Apps zu verwenden. Die iPhone-Nutzer gaben an, die app-spezifischen Einstellungen der Ortungsdienste von iOS zu verwenden, um den Zugriff auf ihren Standort von App zu App selektiv zu erlauben. Während einige Android-Nutzer angaben, den Standortzugriff für Apps dauerhaft aktiviert zu haben, gaben andere an, dazu übergegangen zu sein, den Standortzugriff vor der Nutzung ihrer Apps gezielt an- oder auszuschalten, um ihre Privatsphäre zu schützen. Nur vier Teilnehmer gaben an, den Zugriff auf ihren Standort dauerhaft deaktiviert zu haben. Drei von ihnen begründeten, sie würden nicht von „anderen“ oder Apps überwacht werden wollen. Ein iPhone-Nutzer erklärte hingegen, die Ortungsdienste vollständig ausgeschaltet zu haben, da ihn die Anfragen zur Zugriffserlaubnis der einzelnen Apps gestört hätten.

Neben dem Schutz der eigenen Privatsphäre war das Schonen des Akkus ein häufig genannter Grund für das selektive Deaktivieren des Standortzugriffs. Der durch die Standortfunktionen gebotene Komfort war für viele Nutzer das Hauptargument, diese aktiviert zu haben, auch wenn sie sich überwacht fühlen. Während der Diskussion über genutzte standortbezogene Apps berichteten interessanterweise zwei weibliche Teilnehmer, sie würden die Standortfunktionen ihres Telefons nutzen, um ihren Aufenthaltsort zeitweise von ihren Lebenspartnern überwachen zu lassen, um sich beim späten Ausgehen sicherer zu fühlen.

7.3.1.3 Erfahrungen und Wünsche der Nutzer

Im Rahmen der Diskussion über die momentan gebotenen Standortfunktionen der mobilen Betriebssysteme äußerten die meisten iOS-Nutzer, weitestgehend zufrieden zu sein. Einer von ihnen wünschte sich, eine Übersicht der letzten Standortnutzungen aller seiner Apps zu haben. Diese Funktion existiert schon im Betriebssystem, jedoch zeigt sie nur an, welche Apps „kürzlich“ oder innerhalb der letzten 24 Stunden auf die Ortungsdienste zugegriffen haben. Dies ermöglicht nur eingeschränkt einen Rückschluss darauf, bei welcher Aktion der aktuelle Standort eines Nutzer verwendet wurde. Es dient nur einem groben Überblick. Dem Teilnehmer war diese Funktion gar nicht bekannt. Ein anderer iOS-Nutzer wünschte sich, dass Apps erklären sollten, wieso sie Zugriff auf seinen aktuellen Standort haben wollen, um eine fundierte Entscheidung über die Erlaubnis treffen zu können. Die übrigen Teilnehmer der Gruppe widersprachen ihm. Sie würden der Angabe von Entwicklern über die Nutzung der Standortinformationen nicht vertrauen und daher seien diese nutzlos. Die Android-Nutzer wünschten sich im Allgemeinen mehr Transparenz über die Nutzung ihrer persönlichen Informationen. Einige von ihnen gaben an, dass sie gerne eine Übersicht

hätten, wann welche App ihren Standort zuletzt verwendet hat oder auch wie häufig eine App diese Information erfasst, selbst wenn sie diese Informationen eventuell nicht regelmäßig prüfen würden. Diese Funktion würde ihnen ein sicheres Gefühl in Bezug auf ihre Privatsphäre bereiten. Außerdem würde dies vielleicht dafür sorgen, dass „die Entwickler von Apps mit ihrem Standort verantwortungsvoller umgehen“, gaben einige der Android-Nutzer an. Nachdem die Android-Nutzer gemeinsam mit den iOS-Nutzern diskutiert hatten, wünschte sich mehr als die Hälfte der Android-Nutzer auch die Möglichkeit die Nutzung von Standortinformationen für jede App einzeln bestimmen zu können. Ihnen gefiel insbesondere auch das direkte Feedback des Pop-up-Dialogs, mit dem iOS nach der Berechtigung zur Nutzung der Ortungsdienste für eine App fragt. Die Android-Nutzer klagten in diesem Zusammenhang über die komplexe Einstellungen-App von Android.

Genauigkeit von Standortinformationen Im Rahmen der Diskussion über mögliche Verbesserungen der Kontrolle der Preisgabe von Standortinformationen führte eine Teilnehmerin einer Gruppe das Thema direkt auf die Genauigkeit des preisgegebenen Standortes: Sie stellte fest, dass ihre App *Öffi - Fahrplanauskunft* verständlicherweise ihren genauen Aufenthaltsort braucht, um die nächstgelegene Haltestelle zu finden. Wenn sie hingegen mit einer anderen App nach Rabattcoupon zum Shoppen suche, dann sollte jener App die Angabe ihrer Stadt vollkommen ausreichen. Folglich wären zwei Stufen von Genauigkeit wünschenswert: Genau und ungenau „wie die Stadt in der man sich befindet“ seinen völlig ausreichend, meinte sie. Während ein Teilnehmer einlenkte, dass ihm die Konfiguration damit schon zu kompliziert werden würde, begrüßten die anderen Teilnehmer der Gruppe die ungenaue Standortangabe. Die Teilnehmer gaben an, sie würden überall, wo es möglich sei, die ungenaue Standortangabe verwenden. Innerhalb der Fokusgruppe zeigten sich jedoch verschiedene Vorstellungen der Teilnehmer, welche Genauigkeit die beste Wahl für die ungenaue Angabe sei, wenn sie beispielsweise ein Restaurant in der Nähe suchen oder ihren Standort in einem Facebook-Beitrag angeben würden. Einige stimmten für die Stadt, für andere war schon der Stadtteil recht ungenau und wiederum ein anderer sprach von „auf einen Kilometer ungenau“. Auch in den anderen Fokusgruppen begrüßten die Teilnehmer die Idee der Ungenauigkeit. In einer Gruppe sprachen sich die Teilnehmer deutlich dagegen aus manuell festlegen zu müssen, was ungenau für sie persönlich bedeutet.

Verschleierungsmethoden Am Ende der Gruppendiskussionen wurde versucht, den Teilnehmern das Thema Standortverschleierung näher zu bringen. Ihnen wurden die Konzepte *Verschieben*, *feste Position*, *k-Anonymität* und *adressbasierte Verschleierung* an Beispielen demonstriert. Zudem wurden jeweils die zugrunde liegende Idee und die Wirkung der Methoden grob erläutert.

Die Teilnehmer gaben direkt an, dass die Nutzung selbst bestimmter fester Orte

keine sinnvolle Methode sei. Sie könnte nur dazu dienen, jemandem vorzugaukeln an einem Ort zu sein an dem sie sich gar nicht befinden. Sie argumentierten vor allem auch, dass ein verfälschter Ort einen gewissen Bezug zum wahren Ort behalten muss, wenn man standortbezogene Dienste nutzen möchte. Diese Feststellung betont nochmals, dass andere wissenschaftliche Arbeiten, die zum Ziel haben, die Preisgabe der Informationen zu verhindern, oder die sie durch kontextlose gefälschte Daten ersetzen [74, 76, 110], nicht nutzbar sind, wenn jemand standortbezogene Dienste nutzen will. Das Verschieben des wahren Standortes wurde von den Teilnehmern kritisiert, da die resultierenden Orte „rein zufällig“ seien und die preisgegebenen Orte an einem Ort ohne Bezug zum wahren Ort liegen könnten. Darüber hinaus könnten die preisgegebenen Informationen unglücklicherweise einen sinnlosen, unerwünschten oder fragwürdigen Ort angeben, an dem sie nie gewesen sind. Diese Kritik gilt auch für andere Verfahren, wie das Abschneiden von Nachkommastellen [74].

Die Teilnehmer wiederholten mehrfach, dass ein verschleierter Ort immer einen gewissen Bezug zum wahren Ort behalten sollte. Aus diesem Grund gaben viele Teilnehmer an, die adressbasierte Verschleierung zu bevorzugen, die ihren wahren Ort auf die Mitte der nächstgelegenen Straße abbildet oder alternativ auf das Zentrum des Stadtteils oder der Stadt in der sie sich aktuell befinden. Im Rahmen der Diskussion dieser Methode zeigten sich deutliche Unterschiede zwischen den Fokusgruppen: Eine Gruppe war sich einig, dass es für sie vollkommen akzeptabel wäre, wenn ein Dienst wie Google Maps, welcher sie bei der Verschleierung unterstützt, ihren wahren Standort erfährt, während alle Apps einen verfälschten Ort erhalten würden. Die Teilnehmer einer anderen Gruppe drückten hingegen deutlich aus, dass sie ihren wahren Ort mit keinem einzigen externen Dienst teilen wollen würden, wenn sie die Wahl hätten.

Als die Diskussion auf die grundlegende Idee der k-Anonymität gelenkt wurde, zeigten einige Teilnehmer ein deutliches Interesse am Konzept nicht in einer Menge von k Personen erkannt werden zu können. Sie gaben jedoch alle zum Ausdruck, dass sie einer Verschleierungsmethode gegenüber abgeneigt seien, deren Ergebnis vom Aufenthaltsort anderer Nutzer abhängen würde. Sie verglichen dabei Szenarien, in denen sie spät abends allein unterwegs wären mit dem Besuch von Massenveranstaltungen. Diese Abneigung gegenüber der k-Anonymität ist eine wichtige Erkenntnis, da das Konzept in der Privatsphäre-Forschung recht verbreitet ist.

Fazit der Gruppendiskussionen Die Teilnehmer wünschten sich Kontrollmöglichkeiten, mit welcher Genauigkeit Standortinformationen an ihre Apps preisgegeben werden. Sie unterschieden zwischen den Anwendungsfällen der verschiedenen Apps. Die verschleierten Standortinformationen sollten möglichst ungenau sein. Dabei sollte die entstandene Ungenauigkeit jedoch berechenbar und für sie nachvollziehbar sein. Ein gewisser Bezug zum wahren Ort muss erhalten bleiben.

Unsicherheit beim Vertrauen gegenüber Anbietern In den Fokusgruppen konnten leider keine Muster bezüglich der Wahrnehmung des Vertrauens gegenüber Apps oder Dienstanbietern identifiziert werden. Die Meinungen der Teilnehmer gingen sehr stark auseinander. Es zeigte sich vor allem ein merklicher negativer Einfluss durch die Veröffentlichungen zum Überwachungsskandal des amerikanischen Auslandsgeheimdienstes NSA, die in den Wochen vor der Durchführung der Gruppendiskussionen bekannt wurden.

Als die Android-Nutzer sich speziell über Google äußerten, reichten ihre Aussagen von „Google ist der einzige Anbieter, dem ich vertraue“ bis zu Äußerungen wie „Google weiß sowieso alles über mich, auch wo ich mich aufhalte, selbst wenn ich den Standortzugriff deaktiviere“.

7.3.2 Design und Implementierung

Aufbauend auf den Erkenntnissen der Fokusgruppen wurde eine nutzerfreundliche Standortverschleierung für Android entworfen und implementiert. Die Implementierung ermöglicht, die Genauigkeit der preisgegebenen Standortinformationen für jede App verschieden festzulegen. Ein Nutzer legt für eine App fest, ob diese genaue Standortinformationen erhält, ob sie gar keine Ortsangaben erhält oder ob sie verschleierte Koordinaten entsprechend eines gewählten Detailgrads erhält. Durch die Bereitstellung von Zugriffsstatistiken für Standortinformationen kann der Nutzer erfahren wann und wie häufig eine App seinen Standort erfragt. Durch die Schaffung von Transparenz kann er bewusster über die Verwendung seiner Apps entscheiden. Nutzer, denen die Entscheidung über die Genauigkeit schwerfällt, haben die Möglichkeit sich über einen integrierten Crowddienst anzeigen zu lassen, welche Einstellung andere Nutzer für eine App gewählt haben.

7.3.2.1 Verschleierung der Standortinformationen

Basierend auf den Ergebnissen der Gruppendiskussionen wurden zwei Methoden zur Verschleierung realisiert. Nutzer haben die Wahl zwischen einer dienstbasierten und einer lokalen Methode.

Die adressbasierte Verschleierung wurde gewählt, da auch die Teilnehmer der Fokusgruppen diese als sehr intuitiv und einfach zu verstehen wahrgenommen hatten. Durch kombinierte Adresskodierung, Adressbereinigung und Geokodierung wird der aktuelle Ort des Nutzers auf ein Geoobjekt abgebildet, dessen Wahl die einzig notwendige Konfiguration durch den Nutzer darstellt. Basierend auf den Ergebnissen der Fokusgruppen wurden die Detailgrade *Straße*, *Stadtteil* und *Stadt* realisiert. Aufgrund der Struktur der zugrunde liegenden Geodaten entspricht dabei Stadtteil meist dem nächstgelegenen Dorf in ländlichen Gegenden. Wie beim zuvor beschriebenen Standortprivatsphäre-Framework wird die Geocoder-API von Android

verwendet. Soll Google nicht in die Verschleierung der Standinformationen eingebunden werden, kann die Kodierung alternativ mit einem der freien Geocoder von Bing, Yahoo oder MapQuest/OpenStreetMap durchgeführt werden. Gegenüber anderen Methoden bietet die adressbasierte Verschleierung den Vorteil, dass sie sich an den Aufenthaltsort des Nutzers anpasst. Unabhängig davon, ob sich ein Nutzer in einer Kleinstadt oder in einer Großstadt befindet, bleibt Stadtteil der aktuelle Stadtteil und Stadt die aktuelle Stadt. Bei anderen Methoden wie der k-Anonymität verändert sich die Wirkung festgelegter Parameter häufig in Relation zur Umgebung.

Da ein Teil der Studienteilnehmer eine strikte Ablehnung der Nutzung externer Dienste vertreten hatte, wurde zusätzlich eine lokale Verschleierungsmethode implementiert, die die Standortinformationen auf dem Gerät des Nutzers behält. Um die Implementierung insgesamt schlank und einfach verständlich zu halten, sollte die lokale Methode möglichst die dienstbasierte Methode approximieren. Eine Überlegung war daher eine geodatenbasierte Methode lokal umzusetzen. Aufgrund der Größe der Geodaten und der Komplexität der Suche in den Daten war dies auf den aktuellen mobilen Geräten nicht möglich. Einzig eine Beschränkung der Geodaten auf Städte und eventuell Stadtteile wäre im Rahmen des Möglichen gewesen. Somit hätten nicht alle Detailgrade abgedeckt werden können. Zudem wäre weitere Komplexität durch das Herunterladen passender Geodaten geschaffen worden. Aus diesem Grund wurde trotz der Bedenken mancher Teilnehmer das *Verschieben mit Mindestabstand* als lokale Alternativmethode gewählt. In diesem Fall wird der wahre Ort um einen nach unten und nach oben begrenzten Zufallswert in eine zufällige Richtung verschoben. Da sich einige Teilnehmer gegen das eigenhändige Spezifizieren der Ungenauigkeit ausgesprochen hatten, wurden die in Abschnitt 7.2.4 genannten Metaphern als Alternative evaluiert. Es musste festgestellt werden, dass keine einfachen Metaphern existieren, die über Stadtgrenzen oder Landesgrenzen hinaus einheitlich sind. Die Größe eines Wohnblocks unterscheidet sich zum Teil deutlich von Stadt zu Stadt. Auch die Größe eines Sport-Spielfeldes unterscheidet sich signifikant von Sportart zu Sportart und sogar innerhalb einer Sportart zwischen Verbänden. Somit sind solche Metaphern für die Nutzer nicht eindeutig zu verstehen.

Aus diesem Grund wurde entschieden, die Detailgrade der adressbasierten Verschleierung inklusive ihrer Bezeichnungen wiederzuverwenden. Um die lokale Methode zu verwenden, müssen die Nutzer einmalig die Grenzwerte für die verschiedenen Detailgrade an ihr Verständnis einer Stadt anpassen. Damit sie jedoch keine Zahlen eingeben müssen, wurden zwei alternative Konfigurationsmethoden geschaffen. Über einen Konfigurationsassistenten können die Nutzer mithilfe einer Karte Werte für die Detailgrade Stadt, Stadtteil und Straße bestimmen. Dazu wählen sie zuerst eine für sie repräsentative Stadt aus. Diese wird daraufhin auf einer Landkarte angezeigt. Durch die Auswahl eines Punktes am Stadtrand wird der ungefähre Durchmesser ei-

ner Stadt bestimmt. Auf entsprechende Weise werden die Größe eines Stadtteils und die Länge einer Straße ermittelt, aus denen die Konfiguration für die entsprechenden Detailgrade abgeleitet wird. Durch die Frage nach einem Mindestabstand zum wahren Ort wird die Konfiguration vervollständigt. Alternativ zum Assistenten können die notwendigen Werte für die lokale Methode aus gesammelten Erfahrungswerten der dienstbasierten Methode gelernt werden. Verwendet ein Nutzer vorübergehend die adressbasierte Methode, so werden Abweichungen zwischen wahren und verschleierten Orten für die verwendeten Detailgrade protokolliert. Diese können später als Grenzwerte für die lokale Methode übernommen werden.

7.3.2.2 Nutzerinteraktion

Da die meisten Teilnehmer der Fokusgruppen mit der Nutzerschnittstelle von iOS zufrieden waren oder sich Ähnliches für Android wünschten, wurden die Nutzerinteraktionsmechanismen denen von Apple iOS ähnlich realisiert.

Wenn eine App erstmals auf den Standort eines Nutzer zugreift, öffnet sich ein Pop-up-Dialog und bittet den Nutzer um die Konfiguration des erlaubten Detailgrads der Standortinformationen. Wie Abbildung 7.4a zeigt, kann der Nutzer in diesem Dialog eine der fünf Möglichkeiten von *genau* bis *aus* wählen. Schließt der Nutzer den Dialog ohne eine Entscheidung getroffen zu haben, wird bei einer Standortanfrage kein Ort preisgegeben, bis die Konfiguration getätigt wurde. Durch die für Android typischen Benachrichtigungen wird der Nutzer darauf hingewiesen, dass Privatsphäre-Einstellungen ausstehen. Ist ein Crowddienst konfiguriert, der Informationen über die Einstellungen anderer zur Verfügung stellt, so werden im Pop-up-Dialog die häufigsten Einstellungen anderer Nutzer dargestellt. Für die Darstellung wurden zwei Designvarianten implementiert. Wie Abbildung 7.4a zeigt, können die häufigsten Einstellungen andere Nutzer als Text am unteren Ende des Pop-up-Fensters angezeigt werden. Die Darstellung außerhalb der Wahlmöglichkeiten soll weniger dazu verleiten, schlichtweg eine markierte Option zu wählen und den Dialog erfolgreich aber unüberlegt zu beenden, da die Privatsphäre aktuell nicht Teil des Primärziels des Nutzers ist. Aus demselben Grund ist im Dialog auch keine Option vorausgewählt, so dass der Nutzer aktiv ein Detailgrad wählen muss. Die zweite Designvariante zeigt neben den häufig gewählten Detailgraden eine Bewertung in Form kleiner Sterne an, wie sie häufig für die Darstellung von Nutzerbewertungen in Onlineshops verwendet wird. Für jede vollen 20 % der Entscheidungen anderer Nutzer wird ein Stern neben dem jeweiligen Detailgrad angezeigt.

In der App *Einstellungen* können die Nutzer unter *Standortprivatsphäre* die Einstellungen für Apps anzeigen und verändern. Die in Abbildung 7.4b dargestellte Hauptansicht zeigt eine Übersicht über alle Apps, die bisher auf Standortinformationen zugegriffen haben. Neben dem Namen einer App wird dort durch ein Symbol

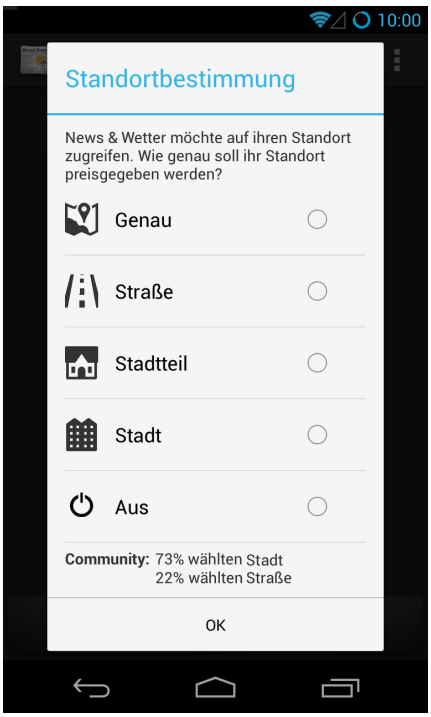
die gewählte Verschleierung angezeigt beziehungsweise ob diese noch zu konfigurieren ist. Durch die Auswahl einer App kann die Konfiguration verändert werden. In den erweiterten Einstellungen kann die Verschleierungsmethode ausgewählt werden. Beim Wechsel der Methode werden die Nutzer über die Unterschiede aufgeklärt. Ist die lokale Methode aktiviert, so können die Werte der Detailgrade manuell oder über die beschriebenen Hilfestellungen bestimmt werden. Die erweiterten Einstellungen erlauben zudem festzulegen, ob ein Nutzer die Einstellungen anderer angezeigt bekommen möchte und ob er selbst seine Einstellungen anonym teilen möchte.

Transparenz Ein besonderes Anliegen vieler Fokusgruppen-Teilnehmer war die Schaffung von Bewusstsein über die Nutzung von Standortinformationen. Um diesem Verlangen nachzukommen, wurden Statistiken über die Standortnutzung implementiert. Abbildung 7.4c zeigt die App-Übersicht der Statistik. Für jede App, die schon einen Standortzugriff gemacht hat, führt sie auf, wann diese den letzten Zugriff auf Standortinformationen genommen hat. Nutzer können die Ansicht nach App-Namen oder nach dem letzten Zugriff sortieren lassen. Durch die Sortierung nach der Anzahl der Standortzugriffe seit der Installation beziehungsweise innerhalb der letzten vier Wochen können Nutzer datenhungrige Apps erkennen. Durch die Auswahl einer App können die Nutzer weitere Details zur Standortnutzung betrachten, wie es Abbildung 7.4d zeigt. Neben der durchschnittlichen Distanz der preisgegebenen Orte von den wahren Orten wird eine detaillierte Statistik über die Standortnutzung der App innerhalb der letzten 24 Stunden und in den letzten vier Wochen angezeigt. Dies ermöglicht dem Nutzer einen Einblick, wie aktiv und regelmäßig eine App seinen Ort verfolgt. Die Statistik enthält keine Informationen darüber, wie aktuell die jeweils preisgegebenen Informationen waren oder welche Orte preisgegeben wurden. Solch eine Historie aufzubauen würde selbst Bedrohungen für die Privatsphäre des Nutzers entstehen lassen.

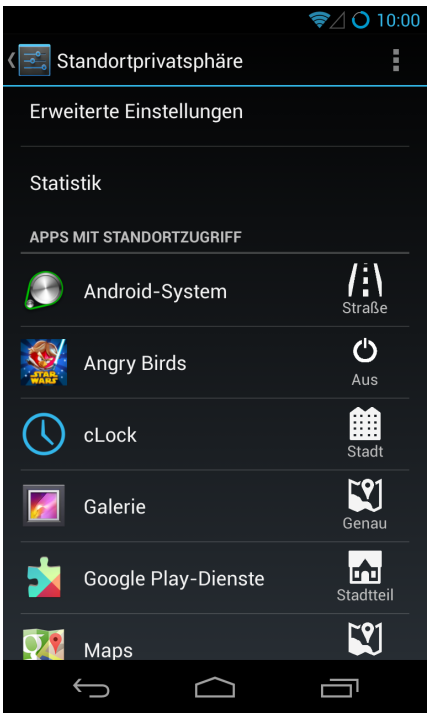
7.3.2.3 Unterstützung der Nutzer bei Standortprivatsphäre-Einstellungen

In den Gruppendiskussionen wurde thematisiert, wie die Teilnehmer die Entscheidung treffen, ob sie einer App den Zugriff auf ihren aktuellen Standort erlauben. Eine Teilnehmerin gab dabei an, sie mache ihre Entscheidung vor allem davon abhängig „wie wichtig ihr persönlich die App ist“ und „wie bekannt der Anbieter der App ist“. Viele andere berichteten hingegen, dies schlichtweg nach ihrem Bauchgefühl zu entscheiden. Um die Privatsphäre-Einstellungen vieler Nutzer nicht allein auf dem eigenen Bauchgefühl beruhen zu lassen, sollte ein Mechanismus gefunden werden, um die Nutzer bei ihrer Wahl zu unterstützen.

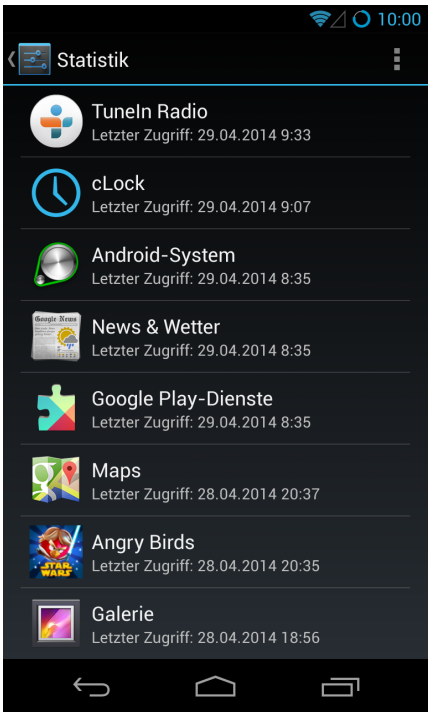
Die meisten Fokusgruppen-Teilnehmer gaben an, sich in der Lage zu fühlen zu entscheiden, welche Apps wie detaillierte Standortinformationen benötigen, um in ihrem



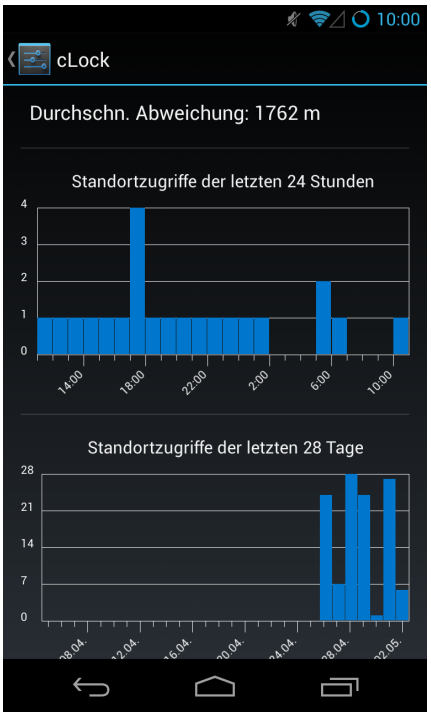
(a) Pop-up-Dialog



(b) App-Übersicht



(c) App-Übersicht der Statistik



(d) Detailstatistik

Abbildung 7.4: Bildschirmfotos der nutzerfreundlichen Standortverschleierung

Sinne angemessen zu funktionieren. Nur wenige Apps empfanden sie als schwierig auf den ersten Blick einzuschätzen: Apps wie die Facebook-App, die verschiedene standortbezogene Funktionen in einer App kombinieren, machen die Wahl schwierig. Alle Teilnehmer gaben an, dass sie niemand anderen ihre Privatsphäre-Entscheidungen treffen lassen würden. Diese Entscheidungen sahen sie klar in ihrer Verantwortung. Einige gaben jedoch an, dass sie im Zweifelsfall jemanden haben, den sie um Rat fragen, wenn sie sich nicht sicher sind. Dies legt die Überlegung nahe, solch einen Rat in Form einer technischen Unterstützungslösung umzusetzen.

In den Fokusgruppen wurden verschiedene Varianten diskutiert, die Unterstützung bieten oder Empfehlungen anderer vermitteln könnten. Eine Variante waren profilbasierte Empfehlungssysteme, die für Profile wie Privatsphäre-Fundamentalisten, Pragmatisten oder Post-Privacy-Nutzer Empfehlungen für die einzelnen Apps aussprechen oder sogar Standardkonfigurationen liefern. Für die diskutierte und implementierte geringe Zahl verschiedener Detailgrade ist die Schaffung differenzierter Profile jedoch kaum möglich. Des Weiteren ist fraglich, ob die letztendlichen Privatsphäre-Entscheidungen der Nutzer mit einer allgemein und einmalig erfassten Privatsphäre-Empfindung übereinstimmen: Ahern et al. [71] hatten beispielsweise im Kontext von Standortinformationen geteilter Fotos deutliche Unterschiede zwischen diesen festgestellt. Eine andere diskutierte Variante war die Schaffung von App-Kategorien, um den Konfigurationsaufwand zu verringern. Läge die Kategorisierung in der Hand des Nutzers, würde dies die konzeptionelle Komplexität der Konfiguration eher erhöhen. Außerdem ist es für viele Apps eher schwierig sie in eindeutige Kategorien einzuteilen, was neue Schwierigkeiten entstehen ließe.

Eine dritte Variante war die Unterstützung der Entscheidung durch eine Online-Community. Einige Teilnehmer waren diesem Ansatz gegenüber abgeneigt, da man solche Empfehlungen fälschen könnte „wie es auch bei Amazon-Bewertungen oder Wikipedia-Artikeln gemacht wird“. Andere begrüßten jedoch die Idee und gaben an, auf diese Weise auch Hilfe zu suchen, wenn es möglich wäre. Eine Gruppendiskussion brachte den Vorschlag hervor, im Rahmen von Sozialen Onlinenetzwerken Empfehlungen zu tauschen. Über die Hälfte der Teilnehmer der Gruppe gab an, im Falle eines solchen sozialen Dienstes auch Geber von Empfehlungen sein zu wollen. Die Übrigen stellten sich als reine Konsumenten dar. Im Kontext der Onlinedienste gaben einige Teilnehmer an, auf Empfehlungen von unabhängigen, gemeinnützigen Anbietern vertrauen zu wollen. Als Beispiele nannten sie die Stiftung Warentest und die Verbraucherschutzzentrale. Auch der Chaos Computer Club wurde in diesem Zusammenhang genannt. Interessanterweise war ein Teil der Teilnehmer bereit, für solche Dienste auch einen geringen Obolus von wenigen Euros zu zahlen. Ein grundlegendes Problem mit den Empfehlungen jeglicher Anbieter ist jedoch, dass diese nur fähig wären, eine begrenzte Menge von Apps wiederkehrend zu prüfen und

zu diesen Empfehlungen auszusprechen. Solange solche Empfehlungen nicht allein auf automatischer Code-Analyse beruhen, bliebe nur die Möglichkeit Empfehlungen etwa für die Top-1000 aller Apps auszusprechen. Genau dieses grenzt jedoch weniger populäre Apps und damit eventuell auch schwer selbstentscheidbare Fälle aus.

Basierend auf den Äußerungen der Teilnehmer wurde für die Implementierung der nutzerfreundlichen Standortverschleierung ein crowdbasierter Social-Web-Dienst entwickelt und integriert. Der Dienst informiert die Nutzer darüber, was andere Nutzer als Einschränkung beziehungsweise Kompromiss zwischen Privatsphäre und Funktionalität für eine App gewählt haben. Darüber hinaus ermöglicht er ihnen, ihre Einstellungen den anderen Nutzern anonym mitzuteilen. Die Fokusgruppen-Teilnehmer hatten signalisiert solch eine Art von Dienst nutzen zu wollen, da sie die Entscheidungen teilweise nicht allein fällen können. Die vermittelten Informationen können dabei als Empfehlung verstanden werden. Sie sollen jedoch nur die Mehrheitsmeinung vermitteln, weswegen diese Informationen nicht für eine Vorauswahl im beschriebenen Pop-up-Dialog verwendet werden. So muss ein Nutzer, wenn auch nur minimal, in Form der Auswahl selbst etwas beitragen. Inwieweit solche Mehrheitsinformationen eher helfen oder auch negativ beeinflussen können, sollte noch weiter untersucht werden. Der Crowddienst bietet den Vorteil, dass durch die Vielzahl der Nutzer die Masse verschiedener Apps besser abgedeckt werden kann. Gleichzeitig ist die Crowd eher fähig auf den alltäglichen Wandel des App-Angebots zu reagieren. Wird eine neue App veröffentlicht und genutzt, so entstehen für sie direkt Einschätzungen. Wie es bei neuen Technologien häufig der Fall ist, können auch bei Apps die häufiger technisch versierten Early-Adopters das Eis brechen und erste Einschätzungen liefern.

Um die Einstellungen anderer anzeigen zu können, muss lediglich ein passender Webdienst konfiguriert sein, der bei jeder Konfiguration der Standortverschleierung konsultiert wird, um die Mehrheitsmeinung daraufhin anzuzeigen. Um eigene Entscheidungen anderen mitzuteilen, sendet Android die Entscheidung eines Nutzers an den Crowddienst, sobald eine neue Einstellung getätigt wurde. Dabei wird der Nutzer über die Google-Play-Dienste via OAuth authentifiziert, um die verschiedenen Nutzer voneinander unterscheiden zu können. Des Weiteren können auf diese Weise nur Besitzer eines Google-Kontos, das Voraussetzung für die Nutzung eines Android-Gerätes beziehungsweise des App-Markplatzes Play Store ist, ihre Einstellungen mit anderen teilen. Die Speicherung der Daten geschieht nach der Authentifizierung vollkommen anonym. Für Nutzer der lokalen Methode werden beim Teilen und Empfangen einer Einstellung zusätzlich die numerischen Entsprechungen der Detailgrade einbezogen, die auf ihren Geräten eingestellt sind. Dies soll verhindern, dass bei völlig verschiedenen Vorstellungen der Größe einer Stadt oder eines Stadtteils ein falsches Bild entsteht. Den Nutzern wird die Möglichkeit geboten, die

numerischen Entsprechungen der Mehrheitsmeinung aus dem Crowddienst auf ihre eigene Konfiguration abbilden zu lassen. Auf diese Weise wird einem Nutzer die Zahlenkonfiguration der anderen in seinen eigenen Worten dargestellt. Der Integrationsmechanismus des Crowddienstes erlaubt auch, einen reinen Empfehlungsdienst zu integrieren. Auf Basis der festgelegten API erkennt er automatisch, ob Informationen nur abgefragt oder auch geteilt werden können.

7.3.3 Fazit

Die Teilnehmer der Fokusgruppen waren an der Verschleierung ihrer Standortinformationen interessiert. Die Diskussionen brachten ein klares Bild hervor, in welchem Detail die Teilnehmer ihre Standortprivatsphäre schützen wollen, welchen Aufwand sie dazu betreiben würden und welche Kriterien sie an die Verschleierung stellen. Sie lehnten die Verwendung komplexer und für sie nicht vorhersagbarer Methoden, wie die k-Anonymität, ab. Sie bevorzugten verständliche Methoden, die einen erkennbaren Bezug zwischen verschleiertem Ort und wahrem Ort erhalten. Einige von ihnen lehnten die Verwendung eines externen Dienstes deutlich ab. Basierend auf den Erkenntnissen der Fokusgruppen wurde eine nutzerfreundliche Standortverschleierung entworfen und implementiert, die eine Verschleierung bietet, die den Wünschen und Anforderungen der Nutzer genügt. Die Verschleierung kann für jede App einzeln festgelegt werden. Die Nutzerschnittstelle erfragt aktiv notwendige Konfigurationen vom Nutzer, ist jedoch nicht sehr aufdringlich. Schwierige Entscheidungen können durch die Ansicht der Entscheidungen anderer unterstützt werden. Statistiken ermöglichen den Nutzern, ein Bewusstsein darüber zu bilden, wann und wie regelmäßig die einzelnen Apps ihren Standort erfassen.

Die Implementierung sollte positives Nutzer-Feedback bekommen, da sie sich stark nach den Vorstellungen der befragten Nutzer richtet. Dies wurde jedoch noch nicht in weiteren Studien und vor allem im Rahmen einer Feldstudie evaluiert.

Offene Aspekte Die präsentierte Implementierung kann einige Probleme nicht lösen, die bisherige Systeme haben. Eines von diesen wurde auch in den Fokusgruppen diskutiert: Den mobilen Systemen fehlt ein Mechanismus, der ein Überdenken einer Privatsphäre-Einstellung erzwingt, wenn sich die Standortfunktionen innerhalb einer App ändern, sich jedoch auf der Ebene der Berechtigungen nichts ändert. Momentan kann solch eine Veränderung der Funktionalität einer App vom Betriebssystem gar nicht erkannt werden.

7.4 Zusammenfassung

Die immense Verbreitung mobiler Geräte, die fähig sind den Ort eines Nutzers zu bestimmen, sorgt für eine ebenso stark verbreitete Nutzung von Apps, die verschie-

denste Funktionen basierend auf dem Standort der Nutzer anbieten. Diese reichen von der Fahrzeugnavigation über die Wettervorhersage zum aktuellen Ort eines Nutzers bis hin zu kostenlosen Spielen, die sich durch integrierte Werbung finanzieren, bei deren Personalisierung auch der Standort eines Nutzers einbezogen wird.

Die aktuellen mobilen Betriebssysteme erlauben den Nutzern teils mehr und teils weniger eine Einflussnahme auf die Preisgabe ihres aktuellen Standortes. Diese Zugriffskontrollen für Standortinformationen dienen dazu, Apps den Zugriff ganz oder gar nicht zu gewähren. Wird ein Standort preisgegeben, so wird dies immer mit vollem Detail getan. Kein System ermöglicht den Nutzern, die Genauigkeit des preisgegebenen Ortes zu beschränken. Dies wäre jedoch wünschenswert für die Wahrung der Privatsphäre, wenn Ortsinformationen mit einer standortbezogenen App genutzt werden sollen, welche gar nicht den genauen Ort eines Nutzers braucht, um korrekt ihren Dienst zu leisten. Durch die Beschränkung der Informationen auf dem Gerät eines Nutzers kann seine Privatsphäre gegenüber einer Vielzahl solcher Apps geschützt werden, da viele von ihnen keine genaue Standortangabe benötigen.

Die Wissenschaft hat seit dem Aufkommen früher mobiler Geräte schon eine Vielzahl von Methoden hervorgebracht, die Ortsinformationen durch eine entsprechende Verschleierung weitestgehend schützen. Trotzdem wurde ein Schutz der Standortinformationen durch Verschleierung von keinem der Betriebssysteme adaptiert. Dies mag diverse Gründe haben, zu denen sicher auch marktwirtschaftliche Überlegungen zählen. Schließlich finanzieren sich viele Apps durch personalisierte Werbung. Einen wesentlichen Grund für die fehlende Adaption liefern die Verschleierungsmethoden jedoch auch selbst: Diese sind oft technisch orientiert und nicht auf Nutzbarkeit getrimmt. Um diesen Missstand zu beheben, wurden zwei Implementierungen geschaffen, die in diesem Kapitel vorgestellt wurden. Ein Framework zur einfachen Integration von Verschleierungsmethoden für Android soll Entwicklern von Verschleierungsmethoden das Erproben ihrer Ansätze in einer realen mobilen Umgebung ermöglichen. Auf diesem aufbauend wurde eine nutzerfreundliche Verschleierung für Android implementiert, die Bedenken und Wünsche von Nutzern berücksichtigt, welche zuvor im Rahmen von Fokusgruppen erhoben worden waren. Diese ermöglicht es, jeder App einen anderen Detailgrad an Ortsinformationen zur Verfügung zu stellen. Einem Teil der Nutzer macht die Wahlmöglichkeit der Genauigkeit vermutlich erst bewusst, dass sie ihren Ort immer maximal genau an Apps und Webdienste weitergeben, auch wenn diese daraufhin nur den Namen einer Stadt anzeigen.

Ein ebenso schwerwiegendes Problem der Verwendung der Standortinformationen auf den aktuellen Systemen ist die fehlende Transparenz, wann der Ort eines Nutzers erfasst wird. Android zeigt nur im Fall von GPS-Ortung an, wenn ein Ort erfasst wird. Apple iOS zeigt dieses bei jeder Form der Ortung an, doch auch hier fehlt dem Nutzer ein Überblick, wie häufig Apps über die Zeit ihren Standort ermitteln und

so etwa ein ungewolltes Bewegungsprofil erstellen. Die Nutzer können daher kein Bewusstsein über die Erfassung ihrer Aufenthaltsorte aufbauen, welches notwendig ist, um fundiert über die Nutzung von Apps zu entscheiden. Die nutzerfreundliche Implementierung widmet sich auch diesem Manko, indem Nutzern eine Übersicht über die vergangenen Standortzugriffe gewährt wird. So schafft sie das notwendige Bewusstsein über die Verwendung der Standortinformationen.

Kapitel 8

Zusammenfassung

Das Bewusstsein von Nutzern über das Vorhandensein und die Preisgabe persönlicher und personenbezogener Informationen ist eine notwendige Voraussetzung, damit die Nutzer ihre Privatsphäre schützen können. Diese Dissertation betrachtete die Problematik des Fehlens dieses Bewusstseins, das die Nutzer daran hindert, ihre Privatsphäre zu wahren. Um die Situation genauer zu erfassen, wurden das vorhandene Bewusstsein sowie mögliche Methoden zur Schaffung von Bewusstsein anhand zweier Anwendungsfälle betrachtet, in denen aufgrund massiver Nutzung vermehrt Bedrohungen für eine Vielzahl von Nutzern entstehen können.

Im Kontext des Social Webs wurde das Teilen von Fotos betrachtet. Insbesondere wurde dabei der Fokus auf die Fotos gelegt, die von Anderen geteilt werden. Werden die Nutzer nicht von anderen Personen oder durch automatische Benachrichtigungen infolge von Personen-Markierungen über solche Fotos informiert, wissen sie meist nicht von dessen Existenz. Folglich können sie ihre Privatsphäre nicht vor Bedrohungen durch diese Bilder schützen. Durch zwei Nutzerstudien wurde dieser Sachverhalt genauer untersucht. Die erste Studie bestätigte, dass das Bewusstsein der Nutzer nicht ausreichend ist. Sie charakterisierte weitere Aspekte wie das Wissen der Nutzer über Bild-Metadaten und evaluierte das Konzept von Privatheitsstufen und Privatsphäre-Kompromissen. Die zweite Studie erfasste das Unbewusstsein der Nutzer über das Ausmaß relevanter geteilter Fotos und Metadaten auf Basis der Fotos ihrer Facebook-Freunde. Anhand der erhobenen Zahlen zeigte die Studie, wie schlecht die Nutzer das Ausmaß der möglichen Bedrohung einschätzen können. Aufbauend auf den betrachteten Privatsphäre-Kompromissen wurden verschiedene Methoden in Form von Dienst-Erweiterungen und Mash-up-Diensten vorgestellt, die die Nutzer bei der proaktiven Suche nach relevanten Fotos unterstützen können, oder die die Nutzer über potenziell relevante Fotos informieren können, nachdem diese geteilt wurden. Die Methoden wurden diskutiert und grundlegend durch Simulation und die Erstellung einer Proof-of-Concept-Implementierung evaluiert.

Das durch die erste Studie erfasste Unwissen über Bild-Metadaten wurde in der vorliegenden Dissertation weitergehend betrachtet. Durch zwei Erhebungen wurde gezeigt, wie heutige Webdienste mit Bild-Metadaten umgehen und wie ausgeprägt das Vorkommen von Metadaten heute in der Praxis ist. Da die Studie und die Erhebungen zeigten, dass die Nutzung von Metadaten heute keine Randerscheinung mehr ist, sondern eine ernstzunehmende Quelle von Bedrohungen, wurde die Schaffung von Bewusstsein auch speziell für Bild-Metadaten betrachtet. In Form einer Webbrowser-Erweiterung wurde eine Methode implementiert die Bewusstsein über die häufig nicht sichtbaren Metainformationen geteilter Bilder schafft. Diese zeigte insbesondere, wie Bewusstsein über eingebettete Metadaten im Moment des Teilens der Bilder geschaffen werden kann. Sie ermöglicht den Nutzern dabei Metadaten zu verändern oder zu löschen, bevor diese mit den Bildern aus ihrem Kontrollbereich ins Web gelangen. Im Rahmen einer Laborstudie wurde gezeigt, wie positiv der Bewusstsein schaffende Effekt und die Möglichkeit der Kontrolle durch die Nutzer unter Laborbedingungen wahrgenommen wurden.

Neben geteilten Bildern und deren Metadaten wurde in dieser Dissertation die Preisgabe persönlicher Informationen im Rahmen der Nutzung kontextsensitiver Dienste betrachtet. Diese werden heute insbesondere auf mobilen Geräten in Form standortbezogener Funktionen genutzt, durch die die Nutzer häufig ihren genauen Standort gegenüber anderen preisgeben. Es wurde eine Erweiterung des mobilen Betriebssystems Android erstellt, um die Entwicklung praktikabler Methoden zur Standortverschleierung und deren Evaluierung auf mobilen Geräten in der Praxis zu unterstützen. Aufbauend auf der Erweiterung und den Ergebnissen von Fokusgruppen-Diskussionen wurde eine nutzerfreundliche Standortverschleierung für Android umgesetzt. Diese schafft Bewusstsein und Transparenz über die Nutzung der Ortsinformationen. Gleichzeitig ermöglicht sie, den Detailgrad preisgegebener Informationen einzuschränken. Somit wird den Nutzern ermöglicht, standortbezogene Dienste zu verwenden und gleichzeitig ihre Privatsphäre bestmöglich zu wahren.

Im Rahmen dieser Dissertation wurden verschiedene Methoden präsentiert, die in den beiden Anwendungsfällen Bewusstsein über persönliche Informationen schaffen können. Zum Teil wurden auch Kontrollmöglichkeiten für die jeweiligen Informationen integriert. Bei den übrigen obliegt dieser nächste Schritt nach der Schaffung von Bewusstsein der zukünftigen Forschung und Entwicklung. Die präsentierten Methoden befassten sich mit verschiedenen Aspekten der Problematik des Fehlens von Bewusstsein über persönliche Informationen: Im Fall geteilter Bilder wurde die Preisgabe durch Andere fokussiert. Im Fall der Bild-Metadaten wurde der Aspekt verborgener Informationen betrachtet sowie die implizite Mitpreisgabe dieser Informationen. Im Fall der standortbezogenen Dienste wurde die gewollte, aber dosierte Preisgabe betrachtet.

Kapitel 9

Ausblick

Die vorgestellten anwendungsfallspezifischen Arbeiten können in weiteren Arbeiten auf andere Anwendungsgebiete übertragen werden. Sie bieten zudem eine Basis, um weitere hier nicht behandelte Aspekte der Gesamtproblematik zu betrachten.

Die präsentierten Untersuchungen und Methoden bieten eine direkte Grundlage für die folgenden fortführenden Arbeiten.

9.1 Bewusstsein und Kontrolle über geteilte Bilder

Weitere Untersuchungen des Bewusstseins der Nutzer Auf Basis der präsentierten Studienergebnisse entstehen weitere Fragestellungen zum Bewusstsein der Nutzer über Bedrohungen durch geteilte Bilder. Ein Ziel weiterer Arbeiten sollte sein zu erfassen, wieso die Facebook-Nutzer die Zahl der Fotos von Freunden als Proxy für das Ausmaß der Bedrohungen so falsch einschätzten. Es stellt sich die Frage, wieso die Nutzer das Ausmaß der Metadaten besser einschätzen konnten und wieso sie Personen-Markierungen besser als Ortsangaben eingeschätzt haben. Über die geäußerten Vermutungen hinaus die Gründe für dies zu finden, kann helfen Methoden zur Schaffung von Bewusstsein zu verbessern. Des Weiteren stellt sich die Frage, wieso weniger als ein Drittel der Nutzer den Apps ihrer Freunde den Zugriff auf ihre Daten zu verbieten scheinen. Die Frage, ob dies beabsichtigt ist oder die Nutzer von der entsprechenden Einstellung – und anderen – nicht wissen, sollte untersucht werden. Allgemein sollte die Wahrnehmung der Nutzer in einem größeren Rahmen erhoben werden, um eine umfassende Grundlage für die Schaffung von Bewusstsein und Aufklärung zu bieten.

Schutz durch Personen-Markierungen In Hinblick auf das ungenügende Bewusstsein über geteilte Fotos ist es verwunderlich, dass die Nutzer gemäß der Studie in Abschnitt 5.4 Personen-Markierungen heute hauptsächlich als Bedrohung der Privatsphäre sehen und nicht als eine Hilfe zu ihrem Schutz. Die Markierungen und die

folgende automatische Benachrichtigung über ein Bild sind laut den Ergebnissen der Studie in Abschnitt 5.3 das häufigste Mittel wie die Nutzer heute von geteilten Fotos erfahren. Neben der Kommunikation zwischen den Nutzern ist es bisher auch das einzige existierende technische Hilfsmittel. Die Gründe für diese Wahrnehmung sollten weiter untersucht werden. Die Forschung sollte im Weiteren betrachten, wie solche manuellen Markierungen verstärkt auch zum Schutz der Privatsphäre genutzt werden können, solange keine anderen Methoden realisiert wurden.

Faktoren von Privatsphäre-Entscheidungen Die in Abschnitt 5.3.7 am Beispiel von Ortsinformationen formulierten Faktoren von Privatsphäre-Entscheidungen sollten detaillierter betrachtet werden. Der Einfluss der einzelnen Faktoren und gegebenenfalls weiterer Faktoren sollte durch Studien erfasst werden. Insbesondere sollte dabei der nationale/kulturelle Aspekt von Privatsphäre-Wahrnehmungen genauer untersucht werden, um Methoden zum Schutz der Privatsphäre an die verschiedenen Bedürfnisse aller Nutzer anpassen zu können.

Weiterentwicklung der App Foto-Privatsphäre-Statistik Auf Basis der in Abschnitt 5.4 verwendeten Facebook-App zur Erfassung von Fotos und Metadaten kann in weiteren Arbeiten ein auf die Privatsphäre fokussierter Browser für Fotos aus dem näheren Bekanntenkreis entstehen. Die für die Statistik verwendete Fokussierung auf Ortsangaben, Personen-Markierungen, verschiedene markierte Orte und Personen oder Anzahl von Kommentaren zu einem Bild kann, statt für die Datenanalyse, auch zur Sortierung und Filterung von Fotos verwendet werden, um relevante Fotos einzugrenzen. Dies könnte die manuell durchgeführte Suche nach relevanten Fotos erleichtern. Neben einer optionalen Analyse von Bildinhalten [155] können so vor allem auch die Metadaten zum Schutz der Privatsphäre eingesetzt werden.

Akzeptanz von Privatsphäre-Kompromissen Im Rahmen dieser Dissertation wurde das formulierte Konzept der Privatsphäre-Kompromisse untersucht und angewendet. Die Erkenntnis über die Wahrnehmung verschiedener Privatheitsstufen aufseiten der Nutzer ist eine vielversprechende Basis für neue Schutzkonzepte, die zumindest dem großen Anteil von Privatsphäre-Pragmatisten einen verbesserten Schutz bieten könnten. Bevor Dienste in der Praxis auf Basis solcher Kompromisse realisiert werden, muss die Wahrnehmung der Nutzer in weiteren Arbeiten in einem größeren Rahmen untersucht werden. Dabei sollte insbesondere betrachtet werden, welche Informationen die Nutzer gegeneinander eintauschen würden und was ihre Beweggründe dabei wären. Da schon beim Vergleich abstrakter und fallspezifischer Kompromisse im Rahmen der theoretischen Betrachtungen deutliche Unterschiede festgestellt wurden, ist eine praxisnahe weitere Evaluierung des Konzepts von Nöten. Dies kann mit einer weiteren Evaluierung des SnapMe-Dienstes kombiniert werden.

Evaluierung des SnapMe-Dienstes Der in dieser Dissertation vorgestellte Dienst SnapMe sollte umfassender evaluiert werden, um die Umsetzbarkeit und den realen Gewinn in der Praxis zu erfassen. In einem ersten Schritt kann dazu eine Feldstudie auf Basis der vorgestellten Proof-of-Concept-Implementierung durchgeführt werden. Die Implementierung in Form einer Facebook-App ist für Feldversuche ausreichend, während darüber hinausgehende Arbeiten einer tiefen Integration in einen entsprechenden Fotodienst bedürften.

Kontrolle über relevante Bilder Im Kontext geteilter Bilder betrachtete diese Dissertation exklusiv die Schaffung von Bewusstsein über relevante Aufnahmen. Folgearbeiten müssen sich darauf aufbauend mit Methoden zur Zugriffserlaubnis und Einflussnahme auf gefundene Bilder anderer Nutzer befassen. Bisher widmeten sich nur wenige Arbeiten dem Thema der Kontrolle über Bilder durch Betroffene. Die Schaffung von Zugriff auf geschützte relevante Bilder ist eine völlig neue Thematik, die aus den Arbeiten dieser Dissertation entsteht.

9.2 Bewusstsein über Metadaten

Evaluierung und Weiterentwicklung der Browser-Erweiterung Die in Abschnitt 6.1 präsentierte Browser-Erweiterung wurde im Rahmen einer Laborstudie evaluiert, in der die Teilnehmer anfangs offen über die Funktionen zur Visualisierung und Kontrolle der Metadaten aufgeklärt wurden, um die Nutzbarkeit der Erweiterung betrachten zu können. Durch dieses Vorgehen konnte der Bewusstsein schaffende Effekt der Erweiterung nur eingeschränkt betrachtet werden. Um diesen korrekt zu erfassen, muss im Rahmen einer Feldstudie untersucht werden, ob die in der Laborstudie beobachteten positiven Effekte auch in der Praxis zu finden sind, ohne die Nutzer zuvor auf die Funktionen zu stoßen. Dabei müssen die verschiedenen Elemente der Browser-Erweiterung evaluiert werden: Es muss betrachtet werden, wie invasiv und effektiv die eingeblendeten Indikatoren sind und wie die Seitenleiste angenommen wird und verbessert werden kann. Die Einstufung der Privatheit der angezeigten Informationen in der Seitenleiste und eine mögliche visuelle Indikation dieser ist ein weiterer Aspekt für Folgearbeiten. Aufbauend auf der Evaluierung der Erweiterung kann die Funktionalität verbessert und erweitert werden. Ist die Nutzerakzeptanz so positiv wie in der Laborstudie, sollten die technisch gegebenen Einschränkungen der Browser-Erweiterung/WebRequest-API gelöst werden. Eine Alternative wäre, die Hochladen-Seitenleiste direkt an den Dateiauswahl-Dialog des Webbrowsers zu koppeln.

Verschlüsselung von Bild-Metadaten In Rahmen der Laborstudie zur Browser-Erweiterung zeigte grob ein Drittel der Teilnehmer, dass sie an Verschlüsselung von Metadaten interessiert wären. Diese würde ermöglichen, die vielseitig nutzbringenden Zusatzinformationen zu erhalten und gleichzeitig das Publikum der Informationen und damit Bedrohungen der Privatsphäre zu beschränken. Der Wille der Nutzer Verschlüsselung zu nutzen und deren Umsetzbarkeit müssen weiter untersucht werden, um zu sehen, ob eine höhere Akzeptanz und Nutzung erreicht werden könnte, als in anderen Fällen wie beispielsweise der E-Mail-Kommunikation, bei der sich die Verschlüsselung bis heute nicht durchsetzen konnte.

Betrachtung weiterer Metadaten Neben Bildern können auch diverse andere elektronische Dokumente Metadaten enthalten, die Bedrohungen für die Privatsphäre der Nutzer verursachen können, da sie persönliche Informationen enthalten. Entsprechend muss auch über diese Informationen Bewusstsein geschaffen werden.

Einen nennenswerten Fall bieten beispielsweise Musikstücke, die Nutzer über den *iTunes Store* der Firma Apple erwerben. Die Metadaten der dort erhaltenen MP4-Dateien enthalten die Apple-ID des Käufers. Gelangen die Dateien aus dem Kontrollbereich des Besitzers, können so Account-Daten verbreitet werden. Geht man davon aus, dass ein Teil der Nutzer ihr zugehöriges Passwort so gewählt haben, dass es leicht auf der beschränkten Tastatur eines iPhones eingegeben werden kann, und dies somit einfacher zu erraten ist, entsteht aus potenziell verbreiteten Apple-IDs sogar eine Bedrohung der IT-Sicherheit.

9.3 Nutzerfreundliche Standortverschleierung

Evaluierung der Umsetzung Da die nutzerfreundliche Standortverschleierung für Android auf den Erkenntnissen der Fokusgruppen beruht, lässt sich vermuten, dass die Umsetzung positiv von den Nutzern aufgenommen werden sollte. Trotzdem muss die Akzeptanz der Standortverschleierung im Rahmen einer Feldstudie evaluiert werden. Verschiedenen Details der Implementierung, wie die Statistiken, der Pop-up-Dialog und die Designvarianten der Visualisierung der Entscheidungen anderer Nutzer müssen dabei evaluiert werden. Die dadurch gewonnenen Erkenntnisse können helfen die Lösung zu optimieren. Es sollte auch betrachtet werden, ob die Entscheidungen Anderer unterstützend für die eigenen Entscheidungen der Nutzer wirken oder ob sie ihre Entscheidungen ungewollt stark beeinflussen.

Crowd-gestützter Privatsphäreschutz Das im Zuge der nutzerfreundlichen Standortverschleierung vorgestellte Konzept zur Unterstützung unentschiedener Nutzer auf Basis eines Crowddienstes sollte weiterentwickelt werden. Bisher werden die Nutzer des Crowddienstes nicht differenziert. Da die Qualität der Informationen des Crowddienstes von der Expertise der Nutzer abhängt, muss diese berücksichtigt werden. Beispielsweise können Nutzer entsprechend ihrer Expertise klassifiziert werden und die Antworten der Nutzer auf Wunsch gemäß ihrer Expertise gewichtet werden.

Die technische Abbildung des verbreiteten „Freunde um Rat fragen“ kann auch in anderen Bereichen des Privatsphäreschutzes oder eventuell auch darüber hinaus sinnvolle Dienste leisten.

Anhang A

Der Mobile Security & Privacy Simulator

Im Folgenden wird der in Abschnitt 5.6.4 verwendete Simulator vorgestellt. Für weitere Details sei auf die dazugehörigen wissenschaftlichen Veröffentlichungen [106, 107] und auf die ausführliche Code-Dokumentation [17] verwiesen.

A.1 Motivation

Die Betrachtung von IT-Sicherheit und Privatsphäre im Kontext mobiler Geräte ist eine komplexe Aufgabe: Die Masse und die Verschiedenheit der Nutzer und ihr jeweiliger persönlicher Kontext sorgen für eine hohe Komplexität betrachteter Fragestellungen. Zudem beherbergt das heutige Ökosystem mobiler und nicht-mobiler Systeme eine große Vielfalt an Geräten, deren Interaktion miteinander und mit den Nutzern ebenfalls für eine Vielzahl zu berücksichtigender Parameter sorgt. Will man Fragestellungen für solch ein System untersuchen, so ist es häufig schwierig, dies rein durch Mathematik zu erfassen.

Eine Möglichkeit Problemstellungen zu erkunden oder neue Konzepte zum Schutz der IT-Sicherheit oder der Privatsphäre nach dem Entwurf zu testen, ist die Durchführung von Laborstudien und umfangreicher Feldstudien. Diese sind jedoch meist zeitaufwändig, teuer und teilweise schwierig in dem Ausmaße durchzuführen, welches für aussagekräftige und repräsentative Ergebnisse notwendig ist. Während Studien zur Evaluierung technischer Systeme und zur Bewertung ihrer Nutzbarkeit unabdingbar sind, sind Szenarien in Größenordnungen von Hunderten oder Tausenden Nutzern kaum kostengünstig zu bewerkstelligen.

Je nachdem, welcher Aspekte der IT-Sicherheit oder Privatsphäre untersucht wird, sind praktische Untersuchungen zudem nicht immer machbar oder ethisch vertretbar. Viele Evaluierungen der Privatsphäre bergen die Gefahr, selbst in die

Privatsphäre von Teilnehmern einzugreifen: Werden Aspekte betrachtet, bei denen man davon ausgeht, dass sie eine Störung der Privatsphäre hervorrufen können, so wirkt diese Störung auch auf die Privatsphäre der Teilnehmer einer Studie. Des Weiteren verlangt die Forschung oft nach mehr Daten, als ein betrachtetes System an sich benötigt oder produziert, um ausgiebige Untersuchungen zu ermöglichen. Dies wirft zum einen organisatorische Schwierigkeiten auf, wenn keine Teilnehmer für eine tiefgreifende Evaluierung gefunden werden können. Zum anderen sind jedoch auch moralische und rechtliche Abwägungen ein im Bereich der Forschung zu berücksichtigender Faktor. Dies gilt auch für die Evaluierung von Sicherheitslösungen, die zum Teil mit dem provozierten oder in Kauf genommenen Vorhandensein von Sicherheitsproblemen einhergehen müssten.

Solche Faktoren machen es der Forschung oft schwer über theoretische Evaluierungen hinaus zu gehen. Theoretische Betrachtungen bergen jedoch den großen Nachteil, dass sie die Realität meist sehr stark vereinfachen und Modelle zugrunde gelegt werden, die teils sehr weit von der Realität entfernt sind. So wurde beispielsweise die Verbreitung von mobiler Schadsoftware durch Methoden der mathematischen Epidemiologie untersucht [81], die zwar die Variable Zeit einbeziehen, die jedoch die Bewegung Infizierter und Gesunder gar nicht berücksichtigen. Andere Arbeiten verwendeten hingegen generierte Bewegungsmodelle, welche jedoch zu signifikant anderen Ergebnissen führen können, als es reale Bewegungen tun [98, 126]. Die Verwendung separater, generierter oder aufgezeichneter Bewegungsprofile ermöglicht darüber hinaus nicht, interaktives Verhalten von Personen zu berücksichtigen, welches auch einen Einfluss auf die Entwicklung eines Szenarios nehmen kann. Ein weiterer Nachteil theoretischer Betrachtungen ist, dass diese die Nutzer oft als gleich annehmen, was zu ungenauen oder praxisfernen Ergebnissen führen kann.

Eine Möglichkeit den beschriebenen Einschränkungen rein theoretischer und rein praktischer Evaluierungen zu begegnen, ist die Verwendung von Simulation. Simulation verwendet auch Modellierung und vollzieht damit eine gewisse Vereinfachung der Realität. Sie ermöglicht jedoch komplexere Szenarien und mehr Parameter zu berücksichtigen, als es viele mathematische Modelle tun. Auf diese Weise ermöglicht sie mehr von der realen Welt zu berücksichtigen, wie beispielsweise Interaktionen und die Umgebung betrachteter Szenarien. Eine Simulation kann mit Nichten praktische Studien ersetzen. Sie erlaubt jedoch, beispielsweise eine Evaluierung von Problemen und Lösungen mit einer Vielzahl von Personen mit geringeren Kosten durchzuführen.

Simulation bietet sich als ergänzendes Werkzeug zu den anderen Methoden an. Sie kann beispielsweise für eine günstige Erstevaluierung neuer Konzepte verwendet werden oder für die gezielte Untersuchung bestimmter Teilaspekte mit großen Nutzerzahlen.

A.2 Umsetzung

Der *Mobile Security & Privacy Simulator* (MoSP-Simulator) wurde im Rahmen von Forschung und Lehre an der Leibniz Universität Hannover entwickelt, um entsprechende Betrachtungen zu ermöglichen. Zum Zeitpunkt der Entwicklung existierte keine andere Simulationslösung die alle gestellten Anforderungen erfüllte.

A.2.1 Design und Funktionsumfang

Der MoSP-Simulator wurde auf Basis von *SimPy*, einem Framework für die ereignisdiskrete Simulation auf Basis von Python, implementiert. Der Simulator selbst wurde ebenfalls als Framework konzipiert, das Anwendern ermöglichen soll, mit grundlegendem Wissen über die Skriptsprache eine Simulation zu programmieren. Gleichzeitig können alle Möglichkeiten der Programmierung genutzt werden, um Anpassungen und Erweiterungen nach Belieben umzusetzen.

Eine einfache MoSP-Simulation besteht aus der modellierten Umgebung, optionalen Monitoren für die Datenausgabe und simulierten Personen und Objekten.

Das Umgebungsmodell der Simulation ist eine zweidimensionale Fläche, in der sich die simulierten Personen und Objekte aufhalten und bewegen. Angelehnt an das Datenmodell des OpenStreetMap-Projektes wird die Umgebung durch Knoten und Wege modelliert. Flächen wie Parks werden als geschlossene Wege modelliert. Personen bewegen sich meist auf dem Straßennetz, das aus Knoten (Wegpunkten) und Wegen besteht. Sie können diese jedoch auch verlassen. Da Distanzen und Nähe in vielen Szenarien eine große Rolle spielen, haben die Wege eine Ausdehnung. Personen laufen je nach gewähltem Wegtyp nebeneinander auf dem Weg oder auf modellierten Bürgersteigen. Zur Beschreibung des Umgebungsmodells wird das XML-basierte Geodatenformat des OpenStreetMap-Projektes verwendet. Dies ermöglicht dem Ersteller einer Simulation, einen Kartenausschnitt der frei verfügbaren Kartendaten des Community-Projektes OpenStreetMap direkt für die Definition seiner Welt zu verwenden. Die Kartendaten definieren das Straßennetz und die individuelle Breite der Wege, die teilweise explizit kartiert ist und sich sonst am Typ einer Straße orientiert.

Neben den Wegen können auch andere Daten aus den Kartendaten verwendet werden. Knoten definieren beispielsweise auch Orte von Interesse wie Cafés, Bars oder Geschäfte, die in der Simulation direkt verwendet werden können. Durch die Verwendung existierender grafischer Editoren für OpenStreetMap-Daten kann ein Umgebungsmodell komfortabel bearbeitet werden. Sämtliche simulierte Personen und Objekte können auf alle Daten des Modells zugreifen. Dies beinhaltet sämtliche Orte von Interesse oder beispielsweise die Namen oder andere Informationen zu Straßen, Parks et cetera.

Die Kartendaten, welche geographische Breiten- und Längenangaben verwenden, um Objekte zu verorten, werden in das UTM-Koordinatensystem transformiert, so dass Längenangaben und Distanzen direkt in Metern gemessen und spezifiziert werden können. Koordinaten werden zentimetergenau angegeben, um Distanzen im Nahbereich für die Simulation von Techniken wie *Near Field Communication* (NFC) zu ermöglichen. Ein Simulationsschritt entspricht einer Sekunde.

Ein Monitor dient der Überwachung und Protokollierung der Simulation. Er kann beispielsweise in regelmäßigen Zeitabständen oder auch ereignisgetrieben Standorte und andere Informationen der simulierten Personen und Objekte ausgeben, Statistiken erzeugen oder die Visualisierung einer Simulation mit Daten versorgen.

Personen können beliebig viele Eigenschaften haben, die ihre Bewegung oder ihre Interaktion individuell beeinflussen. Auf Basis der vorhandenen Implementierung kann sich eine simulierte Person bewegen, sie kann pausieren und die Karte an den Rändern verlassen. Die Bewegung kann dabei zufällig geschehen, so dass sich die Person an jedem Wegpunkt für einen der möglichen Wege zufällig entscheidet. Alternativ können Bewegungen ebenso zielgerichtet bis zu einem vorbestimmten Knoten des Straßennetzes geschehen. Der Ersteller einer Simulation kann auf die vordefinierten Bewegungen und das allgemeine Verhalten einer Person einwirken, indem er die einzelnen vorgefertigten Komponenten der Steuerung erweitert, wie beispielsweise das Denken/Verhalten steuern, Nachrichten empfangen, das Unterbrechen einer Bewegung, das Ermitteln des nächsten Ziels oder das Agieren an einem Wegpunkt. Zur einfachen Modellierung von Verhalten dienen Zustandsautomaten, jedoch können auch komplexere Modelle integriert werden. Eine Person kann mit anderen interagieren, die sich in einer definierten Entfernung befinden. Auf diese Weise können beispielsweise Gerät-zu-Gerät-Infektionen implementiert werden oder der Inhalt eines geschossenen Fotos kann festgestellt werden. Kommunizieren kann eine Person gezielt mit Einzelnen, mit Gruppen, mit allen oder nur Personen in ihrer Nähe. Die bereitgestellten Funktionen wurden dafür geschaffen, Kommunikation nur auf nichttechnischer Ebene umzusetzen. Eine Simulation eines Netzwerkstacks findet bisher nicht statt. Andere Objekte wie Dienste im Internet oder Überwachungskameras können durch bewegungslose Personen ohne Standort implementiert werden.

Simulierte Personen und Objekte können beliebig viele Aktionen definieren. Eine Aktion, die ebenfalls wie eine Person als eigenständiger Prozess in der Simulation implementiert ist, kann verwendet werden, um menschliches Verhalten wie das zufällige Fotografieren unterwegs zu realisieren oder um beispielsweise ein Mobiltelefon zu modellieren, das selbst für sich agieren kann. Aktionen sind eigenständig; die Implementierung der jeweiligen Person kann diese jedoch beeinflussen.

An jeden Knoten des Umgebungsmodells, das heißt an Wegpunkte oder auch an eine kartiere Sehenswürdigkeit, kann ein aktives oder passives Objekt gekoppelt wer-

den, das ein Objekt der realen Welt modelliert. Besucht eine Person einen Knoten, so kann sie mit diesem Objekt interagieren. Passive Objekte implementieren selbst keine Logik, aktive können dies tun. Diese Wegobjekte können verwendet werden, um beispielsweise Gebäude zu simulieren, die Personen betreten und wieder verlassen. Sie können auch einen WLAN-Hotspot modellieren oder eine Überwachungskamera.

Zur Veranschaulichung der Nutzung des MoSP-Simulators zeigt Listing A.1 die Implementierung einer Simulation einer Zombieinvasion, bei der Personen, die sich bis auf einen Meter einem Zombie nähern, selbst zu einem werden. Detailliertere Beschreibungen befinden sich in der Kommentierung des Quellcodes.

Visualisierung Zur Veranschaulichung von Personenbewegungen oder speziellen Ereignissen bietet der MoSP-Simulator eine pyglet-basierte Visualisierung. Diese zeigt die Bewegung der Personen auf einer OpenStreetMap-Karte durch farbige Punkte an. Darüber hinaus können auch Text oder geometrische Primitive auf der Karte eingezeichnet werden, um beispielsweise bestimmte Ereignisse innerhalb der Simulation zu markieren. Ein Monitor innerhalb der Simulation versorgt die Visualisierung mit Daten. Abbildung A.1 zeigt ein Bildschirmfoto der Visualisierung der Simulation aus Abschnitt 5.6.4. Der graue Kreis im „Lakeshore East Park“ markiert die Position und die Reichweite eines aktuell geschossenen Fotos.

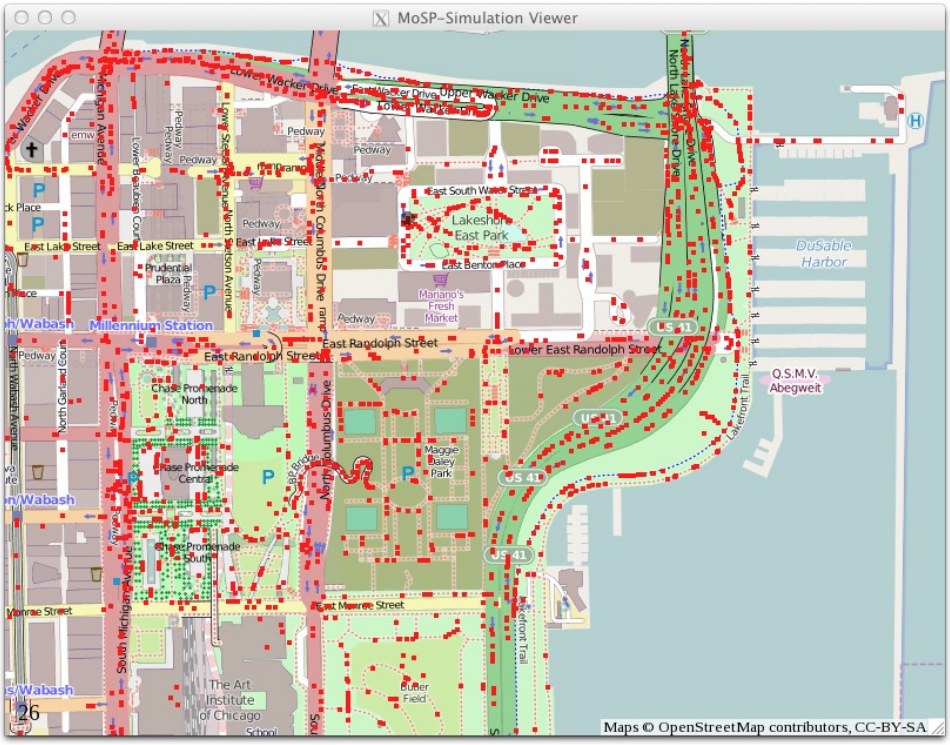


Abbildung A.1: Visualisierung einer MoSP-Simulation

Listing A.1: MoSP-Simulation einer Zombieinvasion

```
class ZombieWiggler(Person):
    """Ein Zombie bewegt sich zufällig und
       infiziert andere in nächster Nähe."""

    def __init__(self, *args, **kwargs):
        super(ZombieWiggler, self).__init__(*args, **kwargs)
        self.p_infected = False
        if kwargs.get('infected'):
            self.infect(True)

    next_target = movement.person_next_target_random

    def infect(self, for_sure=False):
        """Die Infektion

        Wenn nicht infiziert, werde infiziert und schleiche wie
        ein Zombie. Färbe Zombie auf der Karte rot statt blau."""
        if for_sure or self._random.random() < 0.5:
            if self.p_infected == False:
                self.p_infected = True
                self.p_color = 1
                self.p_color_rgba = (1.0, 0.1, 0.1, 1.0)
                self.p_speed = self.p_speed / 2
                start_action(self.infect_other)

    @action(2, start=False)
    def infect_other(self):
        """Die Zombie-Aktion

        Alle zwei Ticks (simulierte Sekunden) wird diese Aktion
        ausgeführt. Es werden alle Personen erfasst, die sich in
        der Nähe von bis zu einem Meter befinden, und daraufhin
        deren Methode infect() aufgerufen. Diese Zombie-Aktion
        ist bei Simulationsstart nicht aktiv. Sie wird durch
        das Infiziertwerden aktiviert."""
        if self.p_infected == True:
            self.get_near(1).call(delay=1).infect(True)

def main():
    """Erstelle eine Simulation

    mit der Karte Hannover; simuliere 60 Sekunden in 1 realen Sekunde
    soweit möglich; gebe Bewegungsdaten über Socket an Visualisierung;
    füge 49 Gesunde und ein Zombie zur Simulation hinzu und zeige sie an;
    das erste Zombie läuft mit 0.7 m/s; simuliere 10.000 Sekunden."""
    s = Simulation(geo=osm.OSMModel('../data/Hannover.osm'), rel_speed=60)
    m = s.add_monitor(SocketPlayerMonitor, 2)
    s.add_persons(ZombieWiggler, 49, monitor=m)
    s.add_persons(ZombieWiggler, 1, monitor=m, args={"infected":True,
                                                     "speed":0.7})
    s.run(until=10000, real_time=True, monitor=True)

if __name__ == '__main__':
    main()
```

Vorverarbeitung von Kartendaten Ein limitierender Faktor der Größe von Karten als Basis für das Umgebungsmodell ist die Anzahl der enthaltenen Wegpunkte, da diese die Größe der notwendigen Routingtabelle für zielgerichtete Bewegungen beeinflusst. Um dieser Begrenzung zu begegnen, wurde das MoSP-GeoTool entwickelt [159, 18], welches die Zahl der Wegpunkte durch Generalisierung verringert. Durch Liniengeneralisierung wird die Zahl der Wegpunkte auf ein mögliches Minimum reduziert, ohne einen großen Detailverlust in Kauf nehmen zu müssen. Die Software ermöglicht darüber hinaus, Partitionen des Straßennetzes zu finden, zu visualisieren und sie zu verbinden. Außerdem können als Knoten kartierte Punkte von Interesse mit dem Straßennetz verbunden werden, um zu diesen routen zu können.

A.2.2 Anwendungsfälle

Neben diversen Beispielszenarien zur Demonstration der Funktionalität des MoSP-Simulators wurde dieser in den folgenden Erstautor-Publikationen verwendet:

In der Publikation zum Simulator [106] wurde die Bluetooth-basierte Verbreitung einer Schadsoftware exemplarisch evaluiert. Im Rahmen der in Abschnitt 5.6.4 vorgestellten Simulation [108] wurde der Simulator verwendet um Nutzer zu simulieren, die Fotos schießen und diese bei einem Webdienst hochladen. Es wurden grundlegende Annahmen zum Identifizieren relevanter Fotos auf Basis von geographischer Kollokation und von Gesichtserkennung geprüft.

Der MoSP-Simulator wurde darüber hinaus in zwei Zweitautor-Veröffentlichungen für die Untersuchung mobiler *Evil-Twin*-Angriffe verwendet [139, 140].

A.2.3 Technische Erweiterungen und Schnittstellen

A.2.3.1 Interaktion mit externen Komponenten

Der MoSP-Simulator implementiert selbst keinen Netzwerkstack für die Kommunikation zwischen den simulierten Personen und Objekten. Diese können jedoch als Client mit externen Netzwerkkomponenten interagieren. Beispielsweise kann durch den Rückgriff auf eine HTTP-Client-Implementierung mit realen Webservern kommuniziert werden, um Daten zu beziehen oder wie in Abschnitt 5.6.4 Fotos bei einem Webdienst zu teilen.

Mit dem Ziel, eine Interaktion zwischen simulierten Nutzern und einer realen Person zu ermöglichen, wurde eine Proof-of-Concept-Implementierung einer externen Bewegungssteuerung für eine simulierte Person entwickelt. Die simulierte Person kann auf Basis von Bewegungsdaten gesteuert werden, die durch eine entsprechende Android-App über das Internet an eine Simulation übermittelt werden. Auf diese Weise befindet sich die simulierte Person genau dort in der simulierten Welt, wo sich die steuernde Person in der realen Welt aufhält.

A.2.3.2 Gekoppelte Simulation

Simulationen des Ökosystems mobiler Geräte sind charakterisiert durch eine Vielzahl von Nutzern, die sich bewegen und miteinander und mit ihrer Umgebung kommunizieren. Um möglichst realitätsnahe Ergebnisse zu erzielen, muss die Umwelt möglichst genau abgebildet werden können. Ein Simulator ist meist nur fähig eine Art von Umgebung bestmöglich und mit einer vorbestimmten Detailtiefe zu modellieren. Der MoSP-Simulator dient beispielsweise vorwiegend der Simulation mit dem Detailgrad von Straßenkarten. Er kann auch Objekte wie ein Café, welches Nutzer betreten oder verlassen modellieren. Die Simulation im Café entbehrt in diesem Fall jedoch jeglichem räumlichen Modell und ist beschränkt auf mathematische Modelle.

Um diesem Umstand zu begegnen, kann ein anderer Simulator für die Simulation innerhalb von Gebäuden verwendet werden. Soll ferner beides, die Bewegung auf einer Straßenkarte und eine Detailsimulation in Gebäuden, vereint werden, so können die Simulatoren miteinander gekoppelt werden.

Um Szenarien zu IT-Sicherheit und Privatsphäre im Inneren von Gebäuden zu simulieren, wurde der *Siafu Kontext-Simulator* erweitert [19], welcher ursprünglich zur Evaluierung kontextsensitiver Anwendungen und Dienste in der zweidimensionalen Fläche geschaffen worden war. Das Umgebungsmodell wurde auf ein 2,5-dimensionales Modell mit Höhenangaben erweitert. So können mehrere Stockwerke modelliert werden. Unter der Berücksichtigung der Raumhöhe ermöglicht der erweiterte Simulator, Funkkommunikation über Stockwerke hinweg zu modellieren. Über Treppen und Fahrstühle können sich die Agenten zwischen Stockwerken bewegen.

Kopplung Mehrere Gebäude-Simulationen können mit einer MoSP-Simulation gekoppelt werden. Der MoSP-Simulator wurde entsprechend erweitert: In der Simulation wird jedes extern simulierte Gebäude durch ein aktives Objekt an einem Wegknoten modelliert. Die Interaktion zwischen den Simulatoren geschieht über Netzwerkkommunikation. Jede MoSP-Siafu-Simulation und die MoSP-Simulation implementieren dazu eine Serverkomponente zur externen Steuerung. Die Steuerung der Simulationen übernimmt ein zentraler Controller. Er synchronisiert die Simulationen anfangs und sorgt für ihr Fortschreiten. Für die Kommunikation, den Transfer simulierter Personen und ein zentrales Logging werden Daten zwischen den Simulatoren und dem Controller im Push- oder Pull-Verfahren ausgetauscht. Der Controller kann dabei die Daten vor der Weitergabe an das jeweilige Ziel in ein entsprechendes Datenformat transformieren. Der MoSP-Siafu-Simulator und die Kopplung der Simulationen werden zusammen mit einer exemplarischen Simulation im Detail in der dazugehörigen wissenschaftlichen Publikation [107] beschrieben.

Anhang B

Weitere Details erhobener Datensätze

B.1 Detailergebnisse der Metadaten-Analyse für Flickr und Locr

Die folgenden Tabellen enthalten detaillierte Ergebnisse der Analyse der Bild-Datensätze aus Abschnitt 5.2.1. Die Felder geben wieder, wie häufig eine Metainformation jeweils enthalten war.

Tabelle B.1 zeigt die Häufigkeiten der Metadaten in den Locr-Datensätzen. Die Daten sind in Anlehnung an Tabelle B.2 in disjunkte Teilmengen aufgeteilt.

Tabelle B.2 zeigt die Häufigkeiten von Metadaten in den Flickr-Datensätzen. Die Daten sind in disjunkte Teilmengen gemäß der Art der Metadatenspeicherung, wie in Abschnitt 5.2.2.2 beschrieben, aufgeteilt.

Tabelle B.3 zeigt die Häufigkeiten von Metadaten in den Flickr-Datensätzen für jede Art der Metadatenspeicherung in absoluten Zahlen.

Spaltenbeschreibung *Ersteller*, *Urheber* und *Kamerabesitzer* zeigen die Menge des Vorkommens von Namen. *ID* zeigt die Häufigkeit von eindeutigen Kameraseriennummern, die von einigen Kameras in die Exif-Metadaten geschrieben werden. Die Spalte *beides* enthält, wie oft Besitzer und Seriennummer gleichzeitig in einem Bild enthalten waren und so eine Kopplung beider Werte herstellten.

Die Spalte *GPS* zeigt, wie viele Fotos Ortsangaben in Form von GPS-Koordinaten enthalten haben. *Ort* zeigt das Vorkommen von textuellen Beschreibungen des genaueren Ortes einer Aufnahme. Dies kann eine Sehenswürdigkeit, ein Stadtteil oder auch eine Adresse sein. *Stadt*, *Bundesland* und *Land* enthalten die Häufigkeit der

entsprechenden Informationen. Die Spalte *Maker* erfasst Ortsangaben, die in speziellen Exif-Maker-Notes gespeichert waren. Da weder eine Online-Dokumentation noch eine entsprechende Kamera verfügbar waren, konnte die Granularität der Angaben nicht genau festgestellt werden. Beispielhafte Bilder von Flickr enthielten Information vom Detailgrad Stadt.

Die Spalte *BBox* (Bounding Box) beschreibt in wie vielen Bildern gespeichert war, wo auf dem Bild eine Person markiert gewesen ist. *Name* zeigt, wie oft Personennamen in diesen XMP-Metainformationen gespeichert waren. Die Spalte *beides* zeigt, wie häufig Markierungen mit Namen zusammen auftraten. Die Spalte *has-people* zeigt, zu wie vielen Fotos die Flickr-API zurückgab, dass Flickr-Nutzer auf einem Bild markiert waren. Die Zahl der Markierungen selbst wurden nicht erfasst. Im Fall der Locr-Datensätze enthält die Spalte Nutzer die Anzahl der Nutzer, die die Bilder des Datensatzes hochgeladen haben.

Die textuellen Ortsangaben in den Flickr-eigenen Metadaten entsprechen den gespeicherten *Where On Earth IDs* [69] der entsprechenden Genauigkeiten. Diese werden von Flickr auf Basis der koordinatenbasierten Ortsangaben eines Bildes ermittelt.

Tabelle B.1: Detailergebnisse der Auswertung der Locr-Datensätze gemäß der Klassifizierung aus Abschnitt 5.2.2.1. Die Zeilen *eingebettete* und *Locr-HTML* enthalten absolute Zahlen, die Zeile *+Locr-HTML* nur die zusätzlichen Metadaten zu der vorherigen Zeile. Die Zeile *verschiedene* beinhaltet eindeutig verschiedene Inhalte.

	Personenangaben					GPS	Textuelle Ortsangaben					Inhalt			Personen-Tags			Nutzer
	Ersteller	Urheber	Kamera Besitzer	Kamera ID	*beides*		Ort	Stadt	Bundes-land	Land	Maker*	Überschrift	Tags	Beschreibung	BBox	Name	*beides*	
Locr-5k-2011 (4.992 Bilder)																		
eingebettete	629	575	450	1072	186	3881	291	297	288	316	5	543	502	396	0	0	0	
+Locr-HTML						1105	2710	2810	3294	4398			407					
Locr-HTML						4986	2892	3045	3556	4706			655					4986
verschiedene	171	155	176	411	119	-	-	-	-	-	-	-	-	-	-	-	-	1772
Locr-25k-2012 (25.201 Bilder)																		
eingebettete	3607	3174	1454	4317	756	14104	2225	2395	2280	2419	17	1979	3206	1555	0	0	0	
+Locr-HTML						11055	14925	15412	16420	21741			5710					
Locr-HTML						25159	16562	17479	18475	24050			57105					25151
verschiedene	419	388	475	954	369	-	-	-	-	-	-	-	-	-	-	-	-	4136

*Ort unbekannter Genauigkeit: herstellerspezifische Metainformation ohne Dokumentation

keine Angabe = Daten nicht verfügbar

Tabelle B.2: Detailergebnisse der Auswertung der Flickr-Datensätze gemäß der Klassifizierung aus Abschnitt 5.2.2.1. Die Zeile *eingebettete* enthält absolute Zahlen, die Zeilen *+extrahierte* und *+Flickr-eigene* geben jeweils nur die zusätzlichen Metadaten zu der/den vorherigen Zeile(n) an.

	Personenangaben					GPS	Textuelle Ortsangaben					Inhalt			Personen-Tags			Flickr API
	Ersteller	Urheber	Kamera Besitzer	Kamera ID	*beides*		Ort	Stadt	Bundes-land	Land	Maker*	Überschrift	Tags	Beschreibung	BBox	Name	*beides*	*getInfo* → *haspeople*
Flickr-20k-2011 (20.836 Bilder)																		
eingebettete	1646	757	182	2511	172	175	53	89	62	84	5	408	848	437	0	0	0	
+extrahierte	1633	1593	660	4565	512	199	34	67	66	93	0	365	627	470	0	0	0	
+Flickr-eigene						3531						16760	11211	11935				470
Flickr-3k-2011-mobil (3.258 Bilder)																		
eingebettete	29	24	6	91	6	363	1	4	2	3	4	76	48	109	0	0	0	
+extrahierte	45	40	12	112	6	564	0	1	0	3	0	56	57	191	0	0	0	
+Flickr-eigene						177						2827	1160	1059				44
Flickr-100k-2012 (100.710 Bilder)																		
eingebettet	6164	4056	1138	15723	1018	2502	245	565	408	483	93	4708	3795	2225	8	11	8	
+extrahierte	6815	4804	1659	13441	1118	2554	175	388	429	525	0	3769	3080	2173	9	10	9	
+Flickr-eigene						7454	3285	8246	8635	8921		80217	39239	24575				681
Flickr-50k-2012-mobil (50.203 Bilder)																		
eingebettete	362	103	0	4	0	6759	25	67	61	68	0	1349	758	1289	4	5	3	
+extrahierte	582	107	0	1	0	12525	16	28	30	34	0	1247	1049	3024	7	9	8	
+Flickr-eigene						959	2214	4272	4410	4458		41639	9797	10454				244
Flickr-50k-2013-mobil (54.086)																		
eingebettete	730	692	0	3	0	21038	65	144	135	142	0	3067	1549	5866	4	5	4	
+extrahierte	158	214	0	0	0	2019	18	42	46	56	0	303	263	913	0	0	0	
+Flickr-eigene						404	3147	5637	5766	5811		34591	25552	7416				139

*Ort unbekannter Genauigkeit: herstellerspezifische Metainformation ohne Dokumentation

keine Angabe = Daten wurden nicht erhoben / Erhebung war nicht möglich

Tabelle B.3: Detailergebnisse der Auswertung der Flickr-Datensätze gemäß der Klassifizierung aus Abschnitt 5.2.2.1. Alle Zeilen enthalten das absolute Vorkommens von Metadaten für die jeweilige Speicherungsart der Daten.

	Personenangaben					GPS	Textuelle Ortsangaben					Inhalt			Personen-Tags			Flickr API
	Ersteller	Urheber	Kamera Besitzer	Kamera ID	*beides*		Ort	Stadt	Bundes-land	Land	Maker*	Überschrift	Tags	Beschreibung	BBox	Name	*beides*	*getInfo* → *haspeople*
Flickr-20k-2011 (20.836 Bilder)																		
eingebettete	1646	757	182	2511	172	175	53	89	62	84	5	408	848	437	0	0	0	
extrahierte	2967	2247	749	6576	744	334	79	141	117	164	0	650	1315	817	0	0	0	
Flickr-eigene						3738						17458	12595	12649				470
Flickr-3k-2011-mobil (3.258 Bilder)																		
eingebettete	29	24	6	91	6	363	1	4	2	3	4	76	48	109	0	0	0	
extrahierte	74	64	12	192	11	916	1	5	2	6	0	121	103	296	0	0	0	
Flickr-eigene						398						2926	1261	1179				44
Flickr-100k-2012 (100.710 Bilder)																		
eingebettete	6164	4056	1138	15723	1018	2502	245	565	408	483	93	4708	3795	2225	8	11	8	
extrahierte	12205	8359	2129	25986	2070	4797	400	894	791	953	0	7688	6513	3949	17	21	17	
Flickr-eigene						9426	3389	8651	9041	9381		85864	45903	27571				681
Flickr-50k-2012-mobil (50.203 Bilder)																		
eingebettete	362	103	0	4	0	6759	25	67	61	68	0	1349	758	1289	4	5	3	
extrahierte	939	208	0	4	0	19076	41	93	91	101	0	2506	1805	4278	11	14	11	
Flickr-eigene						4515	2225	4316	4459	4509		42994	11580	11882				244
Flickr-50k-2013-mobil (54.086)																		
eingebettete	730	692	0	3	0	21038	65	144	135	142	0	3067	1549	5866	4	5	4	
extrahierte	849	895	0	1	0	22653	83	185	180	197	0	2643	1806	4240	4	5	4	
Flickr-eigene						5947	3183	5750	5883	5935		36145	27351	9074				139

*Ort unbekannter Genauigkeit: herstellerspezifische Metainformation ohne Dokumentation

keine Angabe = Daten wurden nicht erhoben / Erhebung war nicht möglich

B.2 Erfasste Geräte der mobilen Flickr-Datensätze

Tabelle B.4 zeigt, welche mobilen Geräte bei der Erstellung der mobilen Flickr-Datensätze betrachtet wurden. Ein *x* in einer Jahresspalte gibt an, dass das jeweilige Kamera-Handy/Smartphone in der Datensatzerstellung des Jahres eingeschlossen war. Auf Basis der IDs wurden folgende URLs durchsucht:

`http://www.flickr.com/cameras_model_fragment.gne?`
`src=js&id=`<*id*>`&category=`<*cat*>,
cat ∈ {*interesting*,*portrait*,*macro*,*night*,*landscape*,*action*,*recent*}

Tabelle B.4: In Flickr-Datensätzen berücksichtigte mobile Geräte

Gerätename gemäß Flickr	Kamera-ID	2011	2012	2013
Apple iPhone 4	72157624172742253	x	x	x
Apple iPhone 4S	72157627469395877	x	x	x
BlackBerry Bold 9700	72157621576215677	x	x	x
BlackBerry Curve 8520	72157616953691070	x	x	x
BlackBerry Curve 8900	72157606582724491	x		
BlackBerry Tour 9630	72157616096845621	x		
BlackBerry Torch 9800	72157623910717049	x	x	x
HTC Desire	72157623390292511	x	x	x
HTC Desire HD	72157624762157476	x	x	x
HTC Droid Incredible	72157623257214966	x	x	x
HTC EVO 4G	72157623237412006	x	x	x
HTC ThunderBolt	72157625411264040	x		
iPhone 3G	72157607254796933	x	x	x
iPhone 3GS	72157620775652629	x	x	x
LG CU720	72157602768624982	x	x	x
LG KF750	72157604583315619	x	x	x
LG KU990	72157601810364683	x	x	x
LG VX-9700	72157605294024642	x		x
Nokia C3	72157623227400843	x	x	x
Nokia E71	72157604507279486	x	x	x
Nokia N8	72157624013405932	x	x	x
Nokia N95	53218	x	x	x
RIM BlackBerry 8530	72157622224883535	x		
RIM BlackBerry 9300	72157623730930449	x		
Samsung Galaxy S	72157623985657132	x	x	x
Samsung Galaxy S 4G	72157625743838619	x	x	x
Samsung Galaxy S II	72157626485419110	x	x	x
Samsung Nexus S	72157626728398240	x	x	x
Sony Ericsson C905	72157605614651448	x		
Sony Ericsson Vivaz	72157622475485570	x		

fortgesetzt …

Gerätename gemäß Flickr	Kamera-ID	2011	2012	2013
Sony Ericsson K800i	261	x	x	x
Sony Ericsson Xperia Arc	72157625577590052	x	x	x
Sony E. Xperia X10 Mini Pro	72157623462273606	x	x	x
DoCoMo D903i	53774		x	x
DoCoMo N905i	72157603345296678		x	x
DoCoMo P905i	72157603328945228		x	x
DoCoMo SH903i	50645		x	x
DoCoMo SO903i	56150		x	x
Helio Fin	72157600767692957		x	x
Helio Ocean	72157600292926652		x	x
HTC Dream	72157607417678583		x	x
HTC Droid Incredible 2	72157625301186015		x	x
HTC EVO Shift 4G	72157624580560158		x	x
HTC Hero	55698		x	x
HTC Hero 200	72157617917812625		x	x
HTC One X+	72157629104662492		x	x
KDDI W21S	1022		x	x
KDDI W42CA	3255		x	x
KDDI W52K	72157600291966813		x	x
LG VX-8550	72157600767694317		x	x
LG VX-9700	72157605294024642		x	x
Motorola Atrix	72157625348586031		x	x
Motorola DROID 3	72157626931643196		x	x
Motorola DROID BIONIC	72157625729544791		x	x
Motorola DROID RAZR	72157627540171397		x	x
Motorola DROID X	72157624455893065		x	x
Nokia Lumia 800	72157627740135087		x	x
Nokia Lumia 900	72157629348324157		x	x
Samsung Epic 4G	72157624297372018		x	x
Samsung Galaxy Ace	72157625948639270		x	x
Samsung Galaxy Nexus	72157627776523729		x	x
Sharp 904SH	1869		x	x
Sharp SX833	650		x	x
Sharp V601SH	5649		x	x
Sharp V902SH	1709		x	x
Sony Ericsson W810i	157		x	x
Sony Ericsson Xperia X8	72157624225311271		x	x
Apple iPhone 5	72157627371520786			x
Apple iPhone 5S	72157631630773540			x
HTC Evo	72157624405761635			x
HTC One	72157632713261880			x
HTC One S	72157629483834391			x

fortgesetzt ...

Gerätename gemäß Flickr	Kamera-ID	2011	2012	2013
HTC One X+	72157629104662492			x
HTC Sensation	72157626485303555			x
HTC Wildfire S	72157626351731908			x
Nokia 808 PureView	72157629112309640			x
Nokia Lumia 920	72157631615124435			x
Nokia N8	72157624013405932			x
Samsung Galaxy Note	72157627762789555			x
Samsung Galaxy Note II	72157632755320446			x
Samsung Galaxy S III	72157629852740322			x
Samsung Galaxy S4	72157633043426867			x
Samsung SGH-I897	72157624356971154			x

Anhang C

Material durchgeführter Studien

Verwendete Begriffe Im Rahmen der Studien wurden zugunsten des Verständnisses der Teilnehmer Begriffe aus dem Volksmund verwendet. So ist im Folgenden mit Sozialem Netzwerk stets ein Soziales Onlinenetzwerk gemeint. Das Soziale Netz wird als ein Synonym für das Social Web verwendet.

C.1 Online-Umfrage zum Bewusstsein über Fotos im Web

Im Folgenden sind alle Fragen des Online-Fragebogens dargestellt. Außerdem ist die Häufigkeit aller Teilnehmerantworten angegeben. Jeder Abschnitt wurde in Form einer neuen Seite im Webbrowser dargestellt, um Fragen inhaltlich zu trennen und um nachträgliche Veränderungen zu vermeiden.

Fragebogen

Willkommen

Willkommen bei unserer Umfrage zum Thema Bewusstsein und Wissen über Fotos im Internet. Diese Umfrage befasst sich mit dem Teilen (Hochladen) von Fotos im Sozialen Netz. Die Umfrage benötigt circa 20 bis 25 Minuten. Unter allen Teilnehmenden verlosen wir zwei Amazon.de-Gutscheine im Wert von je 50 Euro. Um an der Verlosung teilzunehmen, musst du uns am Ende der Umfrage deine E-Mail-Adresse hinterlassen. Die E-Mail-Adressen für die Verlosung werden für keine anderen Zwecke verwendet als die Benachrichtigung der Gewinner. Antworte auf die Fragen spontan.

1. Teilnehmendengruppe – *durch aufrufenden Weblink automatisch ausgefüllt*

Demographische Angaben

2. Bitte gib eine Selbsteinschätzung deiner Computer-Kenntnisse an.

	trifft sehr zu			...			trifft gar nicht zu
Wenn Freunde Computerprobleme haben, fragen Sie mich häufig um Hilfe.	○57	○95	○86	○57	○47	○49	○23
Wenn ich Computerprobleme habe, frage ich häufig meine Freunde um Rat.	○34	○77	○72	○60	○59	○87	○25
	sehr gering			...			*sehr hoch*
Errechnete IT-Expertise	○18	○68	○72	○88	○76	○79	○13

3. Welche Erfahrungen hast du mit folgenden Begriffen im Zusammenhang mit digitalen Fotos?

	kenne ich nicht	habe ich mal gehört	ich weiß was es ist	verwende ich
JPG / JPEG	○2	○6	○27	○379
EXIF	○213	○105	○61	○35
Geotag	○233	○58	○96	○27
DSLR	○261	○74	○40	○39

4. Metadaten sind ...

38○ die Kontrast- und Helligkeitswerte, die in einem digitalen Foto gespeichert werden.
49○ Informationen, die Internetseiten über ihre Besucher und betrachtete Inhalte sammeln.
74○ temporäre Daten, die von einer Digitalkamera zur Bildverarbeitung genutzt werden.
253○ Zusatzinformationen zu einem Foto, wie z. B. Ort, Zeit, enthaltene Personen oder Beschreibung.

5. Bitte bewerte die drei folgenden Aussagen.

	stimme überhaupt nicht zu	stimme eher nicht zu	stimme eher zu	stimme voll zu
Verbraucher haben jegliche Kontrolle über die Erfassung und Verwendung von persönlichen Daten durch Firmen verloren.	○11	○113	○231	○59
Die meisten Firmen behandeln die persönlichen Daten, die sie von Verbrauchern erfassen, angemessen und vertraulich.	○37	○230	○139	○8
Bestehende Gesetze und Geschäftspraktiken bieten heute angemessenen Schutz für die Privatsphäre der Verbraucher.	○73	○248	○91	○2

6. Wie teilst du Fotos mit anderen im Netz?

	nie			...			sehr oft
unterwegs, meist per Mobiltelefon oder Tablet	○188	○89	○26	○23	○40	○18	○30
zuhause, eher am PC oder Laptop	○38	○80	○68	○63	○76	○34	○55

Die Fragen 7 bis 11 wurden nur gefragt und beantwortet, wenn Frage 6 nicht beide Male mit nie beantwortet worden war.

7. Welche dieser Dienste hast du schon für das Teilen von Fotos im Netz genutzt?

354□ Facebook
57□ Google+ / Picasa Web
42□ Flickr
14□ Windows Live SkyDrive
30□ Apple iCloud / Fotostream

8. Wie häufig teilst du Fotos mit anderen im Netz?

190○ weniger als einmal pro Monat
131○ einmal pro Monat
51○ einmal pro Woche
33○ einmal pro Tag
7○ mehrmals am Tag

9. Wenn du ein Foto mit anderen im Netz teilst, lädst du es direkt unterwegs (z. B. per Smartphone) oder erst später hoch?

	nie			...			sehr oft
innerhalb weniger Minuten	○195	○56	○23	○31	○19	○24	○33
innerhalb einer Stunde	○162	○81	○42	○30	○36	○8	○22
innerhalb von 8 Stunden	○105	○76	○57	○64	○40	○13	○26
mehr als 8 Stunden, bis zu Tagen später	○48	○53	○48	○68	○67	○45	○52

10. Welche Personen sind auf den von dir geteilten Fotos zu erkennen?

	nie			...			sehr oft
Ich	○16	○42	○42	○59	○77	○69	○76
Freunde	○21	○45	○48	○64	○84	○74	○45
Freunde von Freunden	○122	○106	○73	○50	○22	○4	○4
Fremde	○188	○118	○29	○25	○9	○6	○6

11. Nach welchen Kriterien entscheidest du, ob du ein Foto im Netz teilst?

	gar nicht			...			sehr stark
Motiv	○2	○1	○2	○30	○71	○97	○178
eigene Bedenken (schadet mir?)	○4	○5	○12	○11	○52	○94	○203
Bedenken anderer (schadet anderen?)	○9	○13	○21	○30	○68	○97	○143

12. Nach welchen Kriterien entscheidest du, wie privat ein Foto für dich ist?

	gar nicht			...			sehr stark
Motiv	○6	○9	○15	○26	○53	○93	○212
Zusatzinformation zum Foto wie Aufnahmeort, Personen, Zeit, ...	○11	○32	○42	○52	○86	○78	○113
Personen, die das Foto sehen können	○3	○9	○8	○28	○46	○112	○208

Bewusstsein über Fotos im Netz

13. Durch Personen-Markierungen bei Facebook, Flickr und Co. kommt man häufig von einem Foto zum persönlichen Profil der Person. Nach einer Markierung wird die Person über die Markierung informiert. Aus welchen Gründen markierst du Personen auf Fotos?

	gar nicht			...			sehr stark
um die Person auf das Foto hinzuweisen	○124	○20	○13	○32	○80	○73	○72
damit Dritte das Foto von der Person finden und sehen können	○227	○55	○35	○44	○25	○14	○14

14. Bewerte das Finden von Fotos durch Personen-Markierungen.

	gefällt mir sehr			neutral			stört mich sehr
Ich finde Fotos, die mich zeigen.	○51	○60	○65	○109	○50	○36	○43
Andere finden Fotos, die mich zeigen.	○6	○23	○47	○132	○65	○57	○84
Ich finde Fotos, die andere darstellen.	○32	○62	○90	○174	○25	○12	○19

15. Wie sehr stört es dich, dass dich andere auf Fotos in Situationen, bei Aktivitäten, an Orten oder mit Personen sehen, wo sie dich nicht sehen sollen?

	stört mich gar nicht			neutral			stört mich sehr
Empfindung	○6	○12	○11	○37	○66	○94	○188

16. Wie groß schätzt du mögliche Folgen ein, wenn andere Fotos von dir zu Gesicht bekommen, die sie nicht sehen sollten?

	sehr gering			neutral			sehr groß
private Folgen	○42	○47	○50	○58	○100	○60	○57
berufliche Folgen	○25	○24	○48	○45	○91	○94	○87
finanzielle Folgen	○99	○85	○64	○76	○50	○19	○21

17. Schätze ein, wie groß eine mögliche Verletzung deiner Privatsphäre durch geteilte Fotos sein kann.
Bei Fotos geteilt von ...

	sehr gering			...			sehr hoch
Freunden	○50	○91	○72	○65	○55	○42	○39
Freunden von Freunden	○24	○21	○46	○84	○99	○73	○67
Fremden	○30	○30	○23	○43	○53	○77	○158

18. Wie erfährst du momentan von Fotos, auf denen du zu sehen bist?

- 76□ Ich suche danach
- 214□ durch Zufall
- 310□ automatische E-Mail nachdem ich als Person markiert worden bin
- 124□ per Nachricht/E-Mail von Freunden
- 19□ per Nachricht/E-Mail von Anderen
- 160□ im Gespräch mit Anderen
- 44□ gar nicht
- 15□ Sonstiges: _____

19. Wie sehr fühlst du dich über alle Fotos im Netz informiert, auf denen du zu sehen bist?

	völlig ausreichend			...			äußerst ungenügend
schöne, angenehme Fotos	○92	○95	○53	○72	○48	○23	○31
ungewollte, unangenehme Fotos	○45	○64	○50	○95	○62	○46	○52

20. Angenommen es würde einen Dienst geben, der dir eine einfache Möglichkeit bieten würde, dich über alle Fotos zu informieren, auf denen du abgebildet bist. Würdest du auch Zeit investieren diese Fotos zu sichten?

- 220○ Ja, auf jeden Fall.
- 173○ Ja, ich wäre interessiert
- 15○ Nein, ich denke der Aufwand wäre mir zu hoch.
- 2○ Nein, ich hoffe alle handeln nach gesundem Menschenverstand beim Teilen von Fotos.
- 0○ Nein, kein Interesse. Mich stört es nicht, wenn andere Fotos von mir im Netz teilen.
- 4○ Sonstiges: _____

Metadaten

Begriffserklärung: Metadaten sind Zusatzinformationen zu einem Foto wie Ort, Zeit, Personen, Beschreibung, Titel, Kontext usw. die mit dem Foto gespeichert werden. Die meisten Digitalkameras fügen grundlegende Metadaten wie z. B. Datum, Uhrzeit und Kameramodell schon beim Fotografieren in ein Foto ein.

Frage 21 wurde nur gefragt und beantwortet, wenn Frage 6 nicht beide Male mit nie beantwortet worden war.

21. Welche dieser Metadaten fügst du zu deinen Fotos hinzu?

	nie			...			sehr oft
Titel / Beschreibung / Schlagworte	○61	○40	○32	○39	○61	○79	○69
Zeitpunkt der Aufnahme	○106	○68	○41	○44	○52	○35	○35
grobe Ortsangabe (Stadt, Region)	○104	○45	○51	○43	○74	○47	○17
genaue Ortsangabe (Adresse, GPS-Koordinaten)	○259	○48	○20	○18	○18	○13	○5
Name des Fotografen	○234	○64	○36	○19	○16	○4	○8
Namen abgebildeter Personen	○94	○48	○50	○54	○79	○33	○23
andere	○200	○44	○18	○86	○18	○9	○6

Frage 22 wurde nur gefragt und beantwortet, wenn Frage 4 (Metadaten sind ...) korrekt beantwortet worden war.

22. Welche Aussagen treffen auf dich zu?

- 64☐ Ich füge keine Metadaten zu Fotos hinzu.
- 91☐ Ich lösche manche Metadaten vor dem Teilen.
- 14☐ Ich lösche alle Metadaten vor dem Teilen.
- 5☐ Mein Fotodienst / Soziales Netzwerk löscht die Metadaten.
- 72☐ Ich weiß nicht, was alles in meinen Fotos steht, wenn ich sie teile.
- 147☐ Ich weiß nicht, was mein Fotodienst / Soziales Netzwerk mit den Metadaten macht.
- 69☐ Ich mache mir keine Gedanken über Metadaten beim Teilen von Fotos.
- 23☐ Gerade beim Teilen im Netz sind Metadaten eine Bereicherung für alle Betrachter.

23. Wie groß schätzt du mögliche Auswirkungen für die Privatsphäre anderer ein, die entstehen könnten, wenn du folgende Metadaten an deine Fotos anfügst?

	sehr gering			...			sehr groß
Titel / Beschreibung / Schlagworte	○87	○122	○60	○73	○34	○21	○17
Zeitpunkt der Aufnahme	○49	○76	○75	○77	○73	○45	○19
grobe Ortsangabe (Stadt, Region)	○34	○52	○77	○79	○100	○52	○20
genaue Ortsangabe (Adresse, GPS-Koordinaten)	○16	○18	○32	○46	○72	○105	○125
Name des Fotografen	○67	○78	○68	○76	○62	○36	○27
Namen abgebildeter Personen	○16	○29	○27	○68	○69	○105	○100

Metadaten – fortgesetzt

24. Wie groß schätzt du mögliche Auswirkungen für deine Privatsphäre ein, die entstehen könnten, wenn andere folgende Metadaten an ihre Fotos anfügen?

	sehr gering			...			sehr groß
Titel / Beschreibung / Schlagworte	○73	○106	○65	○64	○60	○21	○25
Zeitpunkt der Aufnahme	○44	○82	○81	○81	○68	○35	○23
grobe Ortsangabe (Stadt, Region)	○37	○69	○73	○72	○76	○57	○30
genaue Ortsangabe (Adresse, GPS-Koordinaten)	○15	○29	○37	○48	○64	○103	○118
Name des Fotografen	○81	○98	○56	○67	○54	○32	○26
Namen abgebildeter Personen	○26	○43	○40	○56	○67	○94	○88

25. Wie groß schätzt du das Risiko ein, dass jemand auf folgende Weisen irgendwann mal ein Foto findet, welches dich zeigt, er aber nicht sehen sollte.

	sehr gering			...			sehr groß
Du bist im Foto eingezeichnet. Man findet das Foto über dein persönliches Profil.	○101	○79	○36	○45	○53	○50	○50
Dein Name ist im Foto gespeichert. Wer den Namen sucht, könnte es finden.	○46	○79	○48	○55	○73	○62	○51
Du bist abgebildet, aber keine namentliche Nennung. Wer zufällig darauf stößt und dich kennt, erkennt dich.	○45	○85	○68	○73	○67	○46	○30

26. Was empfindest du, wenn folgende Personen Fotos mit zusätzlicher Ortsangabe sehen, auf denen du abgebildet bist?

	stört mich gar nicht			neutral			stört mich sehr
Freunde	○191	○92	○34	○58	○23	○10	○6
Freunde von Freunden	○59	○74	○66	○107	○49	○37	○22
Fremde	○28	○23	○16	○73	○59	○77	○138
der Webdienst, der das Foto speichert	○29	○20	○17	○66	○58	○77	○147
ein Webdienst, der abgebildete Personen sucht und informiert	○31	○17	○25	○62	○42	○73	○164

Abgestufte Privatsphäre

27. Das Soziale Netz lebt vom Teilen von Informationen. Dies beinhaltet auch private Informationen. Es stellt sich die Frage, ob wir alle Informationen gleich stark schützen können. Wollen wir dies überhaupt oder sind manche Informationen weniger privat als andere?
Stufst du alle deine persönlichen Informationen (Aufenthaltsort, Fotos, Metadaten, Freundesliste, Profilfotos, ...) als gleich privat[a] ein oder kannst du dich mit dem Gedanken verschiedener Privatsphäre-Abstufungen anfreunden?

	volle Zustimmung			neutral			absolute Ablehnung
Privatsphäre-Abstufungen existieren	○137	○101	○69	○51	○20	○13	○23

[a] gleich privat = die gleichen oder gleich viele Personen dürfen es erfahren

28. Sind nicht alle persönlichen Informationen zu einem Foto gleich stark privat, kann man sich diese Abstufung zunutze machen: Durch die Nutzung einer weniger privaten Information kann man eine privatere Information schützen.
Beispiel: Gebe einem Dienst z. B. deinen Aufenthaltsort preis, um Fotos zu erhalten, die dort entstanden sind und dich zeigen könnten.
Wie stehst du zu dieser allgemeinen Aussage?

	volle Zustimmung			neutral			absolute Ablehnung
Abstufungen nutzen	○51	○83	○84	○102	○35	○21	○38

29. Bitte schätze folgende Foto-Informationen in Bezug auf ihre Privatheit für dich ein.

	vollkommen öffentlich			neutral		absolut privat	
das Bild selbst	○7	○29	○71	○89	○92	○64	○62
Zeitpunkt der Aufnahme	○18	○30	○84	○89	○122	○38	○33
Name des Fotografen	○41	○49	○71	○97	○71	○48	○37
Eindeutige ID der Kamera	○35	○38	○39	○77	○50	○56	○119
Personen-Markierungen in Foto mit Namen	○1	○12	○34	○36	○106	○115	○110
Personen-Namen ohne Markierung	○4	○13	○45	○61	○113	○92	○86
Objekte auf dem Foto	○26	○77	○75	○117	○68	○29	○22
grobe Ortsangabe (Stadt, Land, ...)	○15	○45	○79	○93	○98	○50	○34
feine Ortsangabe (Adresse, Gebäude)	○3	○5	○9	○29	○59	○120	○189
GPS-Koordinaten	○3	○8	○4	○22	○39	○88	○250
Titel / Beschreibung	○37	○81	○66	○111	○71	○30	○18

30. Welche der folgenden Informationen würdest du deinem Sozialen Netzwerk / Fotodienst anvertrauen, um Fotos von dir zu finden, die du sonst nicht entdecken würdest oder vielleicht gar nicht sehen könntest?

	volle Zustimmung			neutral			absolute Ablehnung
Profilfotos, die bereits schon online sind	○98	○104	○77	○63	○24	○14	○34
weitere Profilfotos, die bestimmte Vorgaben erfüllen, z. B. wie bei Ausweisfotos	○21	○53	○71	○69	○50	○58	○92
meine Freundesliste	○21	○46	○61	○81	○57	○64	○84
zuvor festgelegte Orte auf der Landkarte, an denen ich keine Fotos von mir online haben möchte	○42	○67	○55	○92	○46	○38	○74
meine aktuelle GPS-Position, z. B. per Smartphone-App, in Situationen, in denen ich keine Fotos von mir an dem jeweiligen Orten haben möchte	○16	○31	○32	○50	○37	○52	○196

31. Bewerte folgende Aussage: „Wenn eine beliebige Person den Ort erfährt, an dem ich gewesen bin, finde ich das nicht so schlimm, als wenn die Person private Fotos von mir zu Gesicht bekommt.“

	volle Zustimmung			neutral			absolute Ablehnung
Bewertung	○74	○108	○92	○65	○30	○19	○26

32. Bewerte folgende Aussage: „Wenn mein Soziales Netzwerk den Ort erfährt, an dem ich gewesen bin, empfinde ich das nicht so schlimm, als wenn Freunde und Fremde unerwünschte Fotos von mir zu Gesicht bekommen.“

	volle Zustimmung			neutral			absolute Ablehnung
Bewertung	○71	○102	○77	○67	○36	○28	○33

33. Bewerte folgende Aussage: „Wenn es einen Privatsphäre-Dienst gäbe, der mich über Fotos informiert, auf denen ich unerwünschterweise zu sehen bin, indem ich ihm sage, wo ich gewesen bin, so würde ich ihn nutzen. Ich würde ihm sagen, wo ich war, um die Fotos ansehen zu können.“

	volle Zustimmung			neutral			absolute Ablehnung
Bewertung	○40	○72	○86	○60	○37	○39	○38

Demografische Angaben

34. Dein Alter

Alter	18	19	20	21	22	23	24	25	26	27
Häufigkeit	23	36	54	48	51	40	41	37	16	16
Alter	28	29	30	31	32	33	34	37	39	43
Häufigkeit	14	11	11	2	7	3	1	1	1	1

35. Dein Geschlecht

Geschlecht	männlich	weiblich
Anzahl	223	191

36. Dein höchster Bildungsabschluss

- 1☐ Realschulabschluss
- 281☐ Abitur / Fachhochschulreife
- 15☐ Ausbildung / Lehre
- 13☐ Fachhochschulabschluss
- 101☐ Universitätsabschluss
- 3☐ Promotion

Das bedingte Erscheinen der Fragen 37 und 38 war in der Online-Umfrage nicht korrekt umgesetzt. Daher sind die Antworten auf diese Fragen nicht vollständig. Die gesammelten Antworten zeigen jedoch die diversen Fachrichtungen der Teilnehmer. Da die letztendlich gewählte Zielgruppe Studierende und Mitarbeiter der Universität waren, war Frage 38 zudem nachrangig.

37. Die Fachrichtung deines Studiums

Häufigkeit	**Fächer mit dieser Häufigkeit**
11	Informatik
8	Lehramt an Gymnasien, Wirtschaftswissenschaft
6	Elektrotechnik und Informationstechnik
4	Chemie, Gartenbauwissenschaften, Geschichte, Landschaftsarchitektur und Umweltplanung, Pflanzenbiotechnologie, Physik / Technische Physik / Optische Technologien, Rechtswissenschaften / Europäisches Recht, Sonderpädagogik und Rehabilitationswissenschaften
3	Life Science, Mechatronik

2	Architektur und Städtebau, Bau- , Holz- , Farbtechnik und Raumgestaltung, Bau- und Umweltingenieurwesen, Biologie, Deutsch, Englisch, Geodäsie und Geoinformatik, Geographie, Geowissenschaften, Lebensmittelwissenschaft, Lehramt an berufsbildenden Schulen, Maschinenbau, Mathematik, Politikwissenschaft, Sozialwissenschaften, Wirtschaftsingenieurwesen
1	Biochemie, Bildungswissenschaften, Betriebswirtschaftslehre, Computergestützte Ingenieurwissenschaften, Darstellendes Spiel & Theater, Energietechnik, Lehramt an Grund-, Haupt- und Realschulen, Linguistik, Nanotechnologie, Psychologie, Religionswissenschaft / Werte und Normen, Sozialpädagogik, Volkswirtschaftslehre
112	**Summe**

38. Die Fachrichtung des Abschlusses oder deiner längsten Tätigkeit

Häufigkeit	**Fachrichtung**
70	Naturwissenschaften & Mathematik
43	Technik & Ingenieurswesen
37	Geisteswissenschaft
20	Pädagogik
18	Betriebswirtschaft
16	IT

Anzahl	**Fach**
15	Recht
12	Kaufmännisch
7	Umwelt & Natur
5	Soziales & Heilberufe
4	Handwerk
3	Gestaltung / Design / Kunst
1	Medizin (Human & Tier) inkl. Psychologie
251	**Summe**

C.2 Studie zum Bewusstsein über geteilte Fotos am Beispiel von Facebook

Im Folgenden werden ergänzende Informationen zur Facebook-App *Foto-Privatsphäre-Statistik* und zur dazugehörigen Studie zusammengetragen.

C.2.1 Facebook-App

Im *App-Zentrum* von Facebook wurde die App *Foto-Privatsphäre-Statistik* wie in Abbildung C.1 dargestellt beworben. Beim Starten der App wurden die Nutzer von der in Abbildung C.2 dargestellten Seite begrüßt.

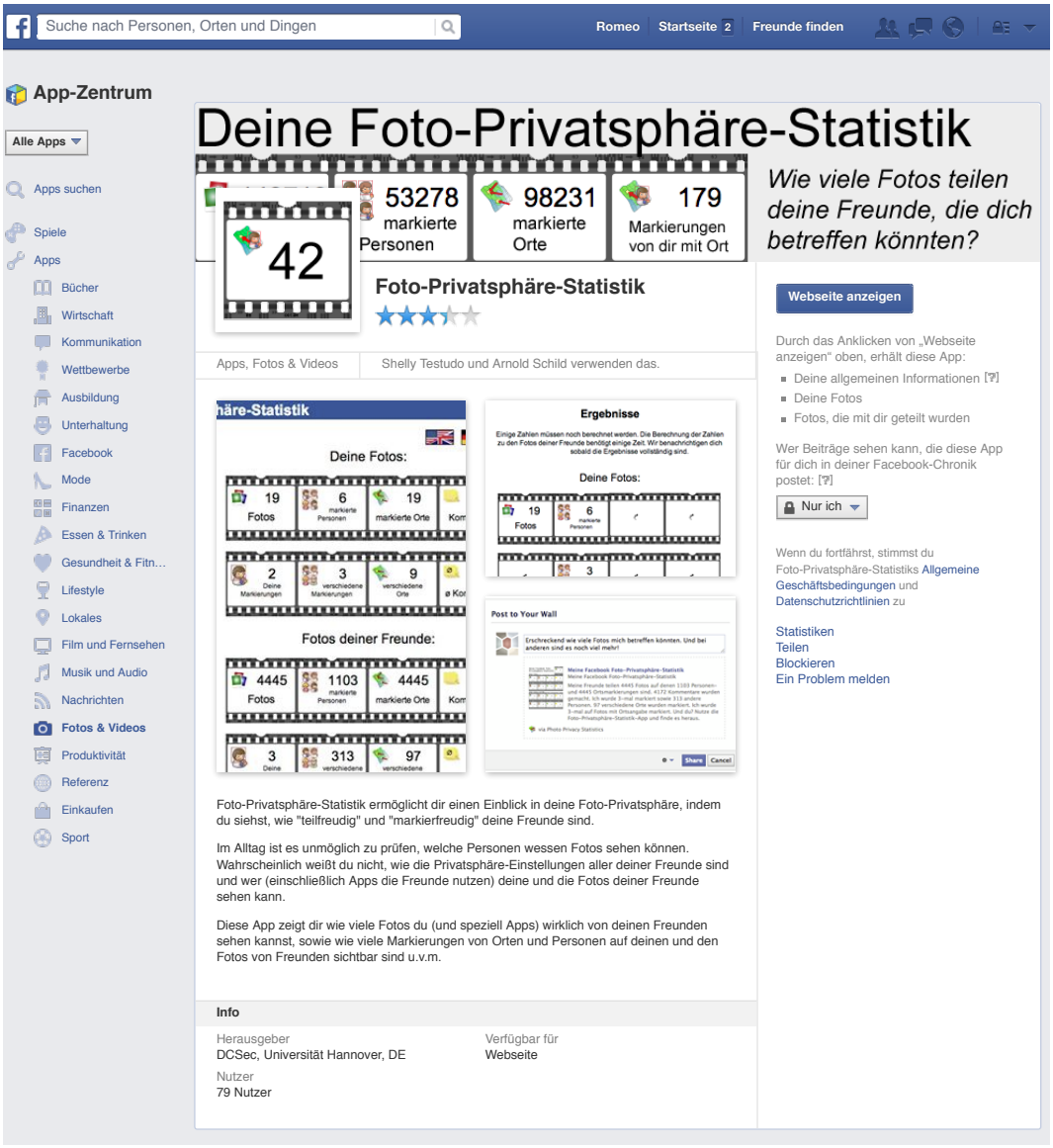


Abbildung C.1: Facebook-App *Foto-Privatsphäre-Statistik* im App-Zentrum

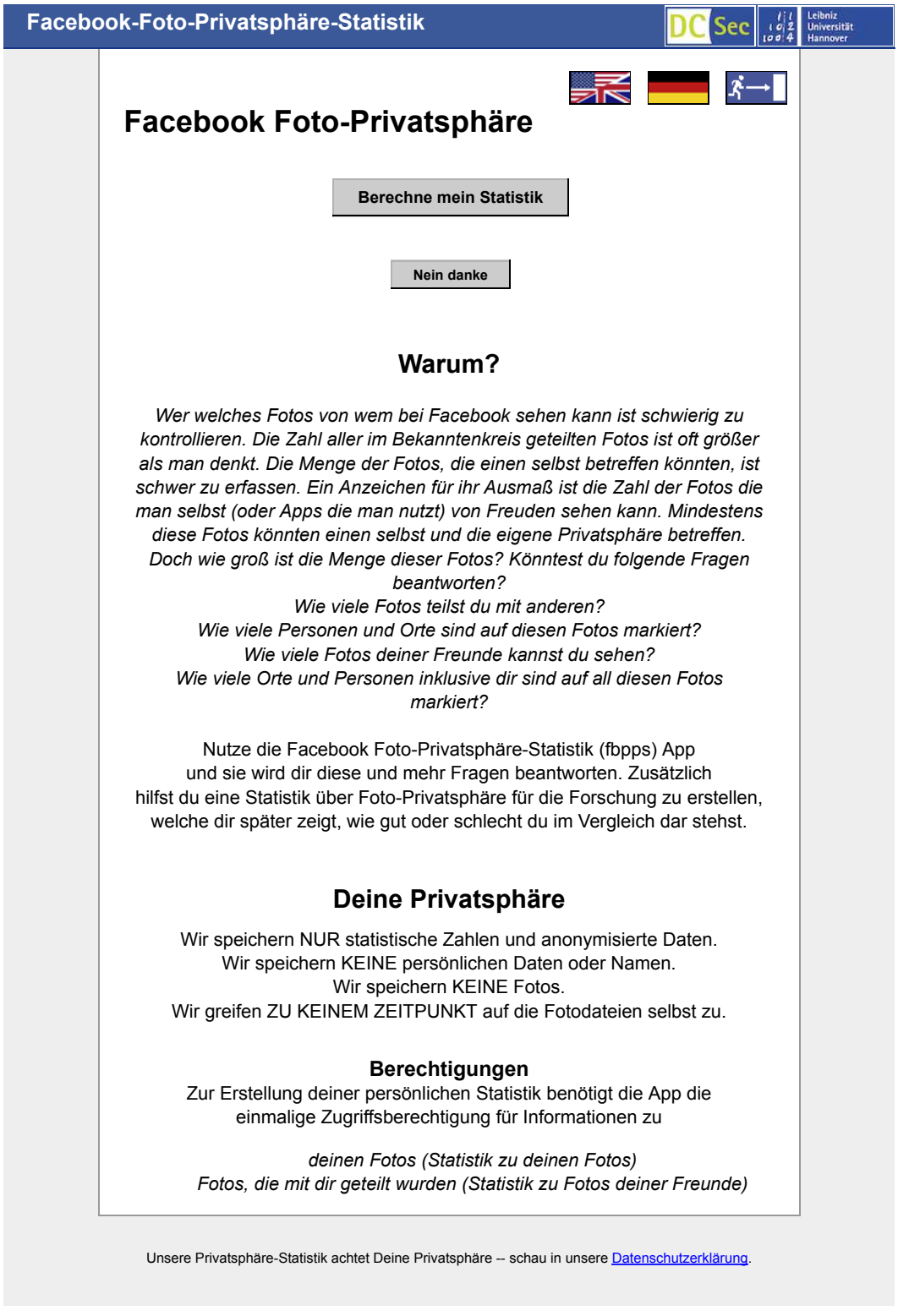


Abbildung C.2: Willkommensseite der Facebook-App

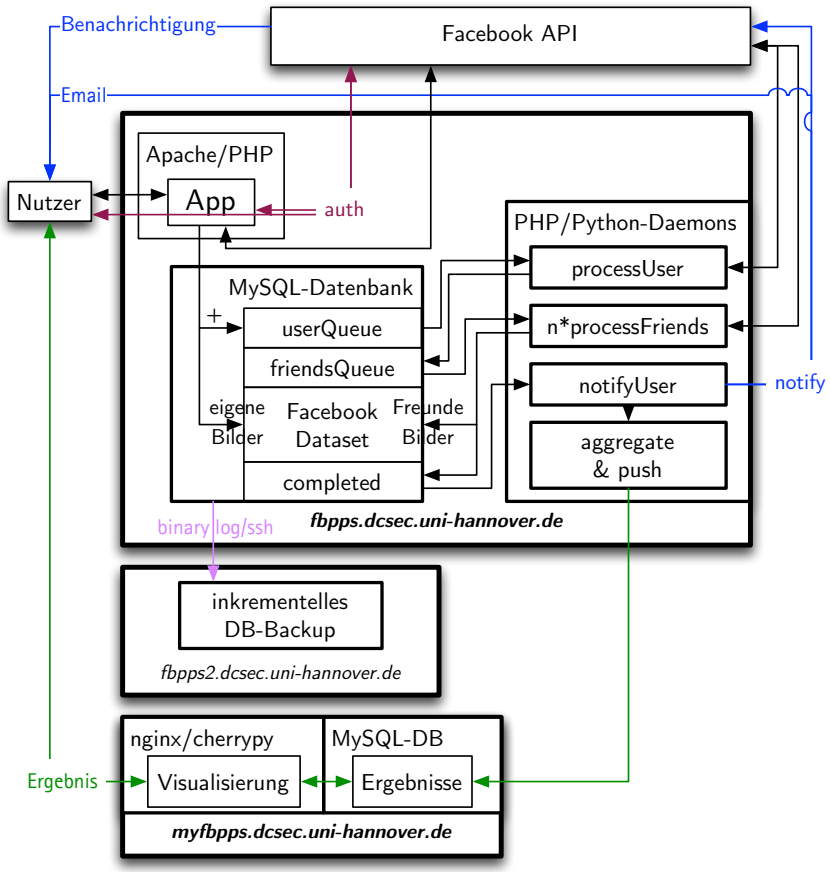


Abbildung C.3: Aufbau der Facebook-App-Infrastruktur

Aufbau und Funktion der Facebook-App

Abbildung C.3 visualisiert den schematischen Aufbau der Infrastruktur der Facebook-App sowie die Datenflüsse bei der Ausführung. Beim Start der App gibt der Nutzer dieser die Berechtigungen für den Zugriff auf seine eigenen Fotos und die Fotos seiner Freunde. Die PHP-basierte App fragt über die Facebook-API die notwendigen Informationen zu den Fotos des Nutzers ab, anonymisiert sie auf Basis von Salted-SHA-1, speichert sie in der MySQL-Datenbank und zeigt die Statistik-Werte zu diesen via AJAX direkt an. Der Nutzer wird mit dem zugehörigen Auth-Token und einer optionalen E-Mail-Adresse in der Datenbank hinterlegt. Sobald ein Hintergrundprozess zur Verfügung steht, werden zu einem Nutzer erst alle Freunde ermittelt und in einem weiteren Schritt zu jedem Freund die Informationen seiner Fotos abgerufen und anonymisiert gespeichert. Wurden alle Freunde abgearbeitet, werden die Statistik-Werte für die Fotos des Nutzers und die seiner Freunde auf Basis der gespeicherten Werte errechnet und an den Server übermittelt, der für die Ergebnisdarstellung zuständig ist. Außerdem werden die Veränderungen am Datenbestand als MySQL-Binary-Log über SSH an einen Backup-Server gesendet, der für

den Fall eines Serverdefekts ein wöchentliches Basis-Backup und alle Inkremente zur Wiederherstellung der Datenbank speichert. Sobald ein Ergebnis an den Ergebnis-Server übermittelt wurde, wird der Nutzer über die hinterlegte E-Mail-Adresse oder über eine Facebook-Benachrichtigung informiert, dass seine Statistik vorliegt. Der Nutzer kann diese nun über einen Link in der Benachrichtigung abrufen.

C.2.2 Pre-Fragebogen

Der Pre-Fragebogen erfragte zu Beginn der Nutzung der App, integriert als HTML-Formular, folgende freiwillig zu beantwortende Fragen. Die Zahlen geben die Häufigkeit der Antworten der 2245 Studienteilnehmer an.

Selbsteinschätzung

Bitte schätze folgende Werte, bevor wir die tatsächlichen Werte errechnen. Der Vergleich von Schätzung und tatsächlichen Werten ermöglicht uns zu sehen, wie gut Facebook-Nutzer über die Fotos, die sie betreffen könnten, Bescheid wissen.

1. Wie viele Fotos aller deiner Freunde kannst du insgesamt sehen?

11○	keine Angabe
502○	keine Vorstellung
92○	unter 50
49○	50
...	{100,200,...900,1.000,...,9.000,10.000,...,90.000,100.000,...,900.000} (Häufigkeit: 115, 81, 62, 49, 107, 30, 22, 22, 22, 235, 115, 56, 51, 129, 17, 21, 27, 12, 169, 77, 41, 15, 29, 10, 4, 8, 3, 38, 10, 3, 4, 5, 1, 1, 0, 0, 0)
0○	1.000.000
1○	über 1 Mio.

2. Wie viele Fotos deiner Freunde haben eine Ortsmarkierung?

50○	keine Angabe
373○	keine Vorstellung
7○	keines
277○	wenige (< 10 %)
426○	jedes zehnte (10 %)
436○	jedes fünfte (20 %)
349○	jedes dritte (33 %)
178○	jedes zweite (50 %)
140○	häufiger (> 50 %)
9○	jedes (100 %)

3. Wie viele Fotos deiner Freunde haben Personen-Markierungen?

63○ keine Angabe
313○ keine Vorstellung
10○ keines
206○ wenige (< 10 %)
262○ jedes zehnte (10 %)
363○ jedes fünfte (20 %)
380○ jedes dritte (33 %)
313○ jedes zweite (50 %)
318○ häufiger (> 50 %)
17○ jedes (100 %)

4. Wie viele Personen sind *im Schnitt* auf einem Foto mit Personen-Markierung(en) markiert?

89○ keine Angabe
404○ keine Vorstellung
132○ 1
689○ 2
... {3,4,5,6,7,8,9} (Häufigkeit: 622, 141, 86, 21, 12, 11, 3)
14○ 10
21○ mehr

5. Durch Personen-Markierungen erfährst du von Fotos, die von dir gemacht wurden. Empfindest du es als Privatsphäre-Vorteil auf Fotos markiert zu werden?

261○ keine Angabe
422○ nein – es ist eine große Bedrohung meiner Privatsphäre
433○ nein – es ist eine mittlere Bedrohung meiner Privatsphäre
249○ nein – es ist eine geringe Bedrohung meiner Privatsphäre
572○ neutral
154○ ja – es birgt geringe Vorteile für meine Privatsphäre
101○ ja – es birgt mittelmäßige Vorteile für meine Privatsphäre
53○ ja – es birgt schlagkräftige Vorteile für meine Privatsphäre

6. Bitte nenne uns dein Alter (für die Statistik). Wir fragen dich an dieser Stelle nach deinem Alter und benötigen so keinen Zugriff auf deine detaillierten persönlichen Daten bei Facebook.

187○ keine Angabe
9○ 13
... {14,...,98}
0○ 99

Alter	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Häufigkeit	9	4	14	35	27	45	43	59	72	87	84	89	90	97

Alter	27	28	29	30	31	32	33	34	35	36	37	38	39	40
Häufigkeit	84	89	85	79	88	69	64	59	62	50	55	47	43	41

Alter	41	42	43	44	45	46	47	48	49	50	51	52	53	54
Häufigkeit	36	39	32	34	22	34	17	36	18	13	16	11	11	13

Alter	55	56	57	58	59	60	61	62	63	64	67	76	77
Häufigkeit	10	6	6	6	3	3	4	4	2	7	3	1	1

C.2.3 Post-Fragebogen

Zum optionalen Post-Fragebogen wurden die App-Nutzer in der Ergebnisbenachrichtigung und auf der Ergebnis-Webseite eingeladen. Die Fragen 3–5 wiederholen Fragen aus der Online-Umfrage in Anhang C.1 mit sprachlichen Optimierungen. Ein Vergleich der Ergebnisse erfolgt in der Diskussion der Ergebnisse dieses Fragebogens.

Facebook Foto-Privatsphäre-Statistik – freiwillige Abschlussfragen

Dieser kurze Fragebogen stellt einige freiwillige zusätzliche Fragen nach der Nutzung der Facebook-App Foto-Privatsphäre-Statistik. Wir hoffen dir hat die App gefallen. Wir würden uns freuen, wenn du dir wenige Minuten Zeit nimmst, um die Fragen zu beantworten.

1. Hättest du solche Zahlen zu den Fotos, die deine Freunde teilen, erwartet?

	viel geringer als erwartet			wie erwartet		viel höher als erwartet	
Anzahl Fotos	○16	○23	○43	○40	○57	○41	○49
Anzahl Personen-Markierungen	○13	○35	○44	○47	○58	○38	○34
Anzahl Ortsangaben	○18	○39	○46	○64	○47	○30	○25
Anzahl Kommentare	○12	○48	○41	○68	○49	○21	○30

2. Beschreibe deine Empfindung über die wirklichen Zahlen auf der Skala von sehr erschüttert bis sehr begeistert.

	sehr erschüttert			neutral			sehr begeistert
Empfindung über Zahlen	○11	○15	○50	○149	○32	○8	○4

3. Wie häufig markierst du Personen aus folgenden Gründen?

	überhaupt nicht			...			sehr häufig
Aufmerksamkeit der/des Markierten auf Foto lenken	○98	○35	○15	○23	○18	○10	○15
andere Personen auf das Foto der Person hinweisen	○115	○39	○9	○20	○21	○4	○6

4. Bewerte die folgenden verschiedenen Auswirkungen von Personen-Markierungen.

	gefällt mir sehr			neutral			gefällt mir gar nicht
Ich finde Fotos, die mich zeigen.	○28	○24	○30	○40	○13	○19	○40
Andere finden Fotos, die mich zeigen.	○2	○18	○30	○44	○33	○19	○48
Ich finde Fotos, die andere darstellen.	○21	○37	○35	○66	○13	○8	○14

5. Wie gut fühlst du dich über Fotos <u>überall im Web</u> informiert, auf denen du zu sehen bist?

	völlig ausreichend			...			äußerst ungenügend
schöne, angenehme Fotos	○13	○24	○28	○28	○37	○33	○48
ungewollte, unangenehme Fotos	○9	○9	○19	○27	○36	○44	○67

6. Wie empfindest du die Privatheit folgender Arten von Daten, wenn Nicht-Freunde/Dritte diese sehen können?

	vollkommen öffentlich			...			absolut privat
Ortsangaben	○21	○12	○19	○23	○37	○30	○77
Personen-Markierungen	○16	○8	○19	○31	○39	○34	○72
Kommentare zu Fotos	○18	○17	○30	○30	○25	○29	○70

7. Gäbe es einen Facebook Privatsphäre-Dienst, welcher Fotos von dir finden kann, die andere geteilt haben, würdest du diesem die Nutzung deines Profilfotos erlauben?

	volle Zustimmung			neutral			absolute Ablehnung
Profilfoto-Nutzung erlauben	○20	○34	○33	○25	○18	○20	○66

8. Gäbe es einen Facebook Privatsphäre-Dienst, welcher andere Personen über Fotos informieren kann, die an für diese Personen privaten Orten gemacht worden sind, würdest du dem Dienst die Nutzung der Ortsangaben deiner Bilder erlauben?

	volle Zustimmung			neutral			absolute Ablehnung
Ortsangaben-Nutzung erlauben	○12	○11	○29	○31	○22	○30	○75

C.3 Laborstudie zur Browser-Erweiterung für Bild-Metadaten

Der folgenden Abschnitt enthält das Material der durchgeführten Laborstudie.

C.3.1 enthält den Online-Fragebogen, der zur Planung der Laborstudie und zur Einschätzung der Teilnehmer verwendet wurde. Die Darstellung zeigt die Häufigkeiten der verschiedenen Antworten der 62 Teilnehmer.

C.3.2 zeigt die Begrüßung der Teilnehmer zur Laborstudie. Der Text wurde zu Beginn jedes Studiendurchgangs vorgetragen.

C.3.3 zeigt die Aufgabenbeschreibung, die an alle Teilnehmer zusammen mit dem Papier-Fragebogen ausgegeben wurde.

C.3.4 enthält den Papier-Fragebogen inklusive der Häufigkeiten der Antworten der 43 Laborstudienteilnehmer.

C.3.5 umreißt die im Rahmen der Studie verwendeten Bilder.

Die Aufgabenbeschreibung und die Einleitung des Papier-Fragebogens enthalten alle Informationen, die die Teilnehmer zur evaluierten Erweiterung des Webbrowsers im Vorfeld erhalten haben.

Die Browser-Erweiterung wurde für die Laborstudie um eine Logging-Funktion ergänzt: Alle Nutzeraktionen wie das Hochladen einer Datei, das Löschen, Ändern oder Verschlüsseln von Metadaten wurden für die spätere Auswertung protokolliert.

C.3.6 zeigt exemplarisch ein auf das wichtigste gekürzte Aktionsprotokoll eines Studienteilnehmers.

C.3.1 Online-Fragebogen zur Teilnehmer-Rekrutierung

Willkommen

Wir suchen Teilnehmende für eine Nutzerstudie zum Teilen von Fotos im Web. Die Studie findet bei uns vor Ort in der Schloßwender Straße 5 im RRZN gegenüber dem Conti-Campus statt und benötigt pro teilnehmender Person 20 bis 30 Minuten. Alle Teilnehmenden bekommen für ihre Teilnahme eine Aufwandsentschädigung von jeweils 5 Euro. Die Studie findet am Mittwoch, dem 16.10. und am Freitag, dem 18.10.2013 statt.

Die folgende kurze Umfrage dient der Studienplanung. Daher fragen wir grundlegende demographische Informationen ab, Termine an denen du Zeit hast sowie Kontaktinformationen für deine persönlichen Einladungen. Zwei bis drei kurze Fragen dienen zuletzt der Erfassung deines Vorwissens.

Wir danken dir jetzt schon für dein Interesse.

Demografische Angaben

1. Dein Alter

Alter	19	20	21	22	23	24	25	26	27	29	30	31	33	34
Häufigkeit	2	4	6	9	6	6	8	9	3	2	2	2	2	1

2. Dein Geschlecht

Geschlecht	männlich	weiblich
Anzahl	22	40

3. Deine Studienrichtung

Häufigkeit	**Fächer mit dieser Häufigkeit**
6	Maschinenbau, Wirtschaftswissenschaften
4	Bau- und Umweltingenieurwesen, Englisch, Pädagogik, Wirtschaftsingenieurwesen
3	Chemie, Jura, Lehramt
2	Architektur, Deutsch, Life Science, Mathematik, Mechatronik
1	Elektrotechnik, Energietechnik, Geodäsie und Geoinformatik, Geowissenschaften, Geschichte, Informatik, Landschaftsarchitektur, Lebensmittelwissenschaften, Musik, Nanotechnologie, Pflanzenbiotechnologie, Politikwissenschaften, Sozialwissenschaften, Sport, Technisch Informatik
62	**Summe**

4. Deine E-Mail-Adresse für die Einladung zu deinem Termin.

5. Optionale Telefonnummer für kurzfristigen Kontakt.

6. Die Studie soll über 2 Tage verteilt stattfinden. Alle Teilnehmenden sollten jeweils 30 Minuten Zeit mitbringen. Für Übergänge etc. sind Zeiträume von je 45 Minuten geplant. Bitte tragt hier ein, zu welchen Zeiten ihr könnt. Wir werden entsprechend eurer Antworten die Zeiten dann schnellstmöglich verteilen und euch benachrichtigen.

Meine Erfahrung

7. Ich habe schon einmal Fotos auf diesen Webseiten geteilt:

57☐ Facebook
10☐ Google+ / Picasa Web
1☐ Flickr
2☐ Windows Live SkyDrive
5☐ Apple iCloud / Fotostream
10☐ private Webseite (mit Galerie-Software)
4☐ Andere: Dropbox
4☐ Andere: StudiVZ
3☐ Andere: Instagram
2☐ Andere: MySpace

8. Metadaten sind ...

3○ die Kontrast- und Helligkeitswerte, die in einem digitalen Foto gespeichert werden.
11○ Informationen, die Internetseiten über ihre Besucher und betrachtete Inhalte sammeln.
5○ temporäre Daten, die von einer Digitalkamera zur Bildverarbeitung genutzt werden.
43○ Zusatzinformationen zu einem Fotos, wie z. B. Ort, Zeit, enthaltene Personen, Beschreibung.

9. Welche Aussagen treffen auf dich zu?

12☐ Ich füge keine Metadaten zu Fotos hinzu.
7☐ Ich lösche manche Metadaten vor dem Teilen.
4☐ Ich lösche alle Metadaten vor dem Teilen.
22☐ Ich weiß nicht, was alles in meinen Fotos steht, wenn ich sie teile.
25☐ Ich weiß nicht, was mein Fotodienst / Soziales Netzwerk mit den Metadaten macht.
14☐ Ich mache mir keine Gedanken über Metadaten beim Teilen von Fotos.

C.3.2 Begrüßung und Informationen zur Laborstudie

Willkommen zu unserer Studie zum Teilen von Fotos im Web

- Ein Durchlauf dieser Studie sollte zwischen 20 bis 30 Minuten dauern. Wir haben insgesamt 45 Minuten bis die nächsten Probanden da sind.
- Zum Ablauf: Nach der Einführung durch mich bearbeitet ihr Aufgaben am PC und beantwortet dazu Fragen auf einem Papier-Fragebogen. Eine Aufgabenbeschreibung leitet euch entsprechend durch die Studie.
- Am Ende kommt ihr – falls andere noch arbeiten – leise zu mir, gebt die Zettel ab, unterschreibt eine Quittung und erhaltet eure 5 Euro.
- Bei Fragen gebt einfach kurz ein Zeichen und ich komme. Lasst bitte die anderen neben euch in Ruhe weiterarbeiten.
- Vor euch sollte nun Folgendes zu finden sein: ein Stift, der Bogen *(1) Aufgabenbeschreibung* und der Bogen *(2) Fragebogen*

Gibt es soweit Fragen?

Nun ein paar Worte zum Thema der Studie

Ich lese diese vor, damit alle Teilnehmenden genau das Gleiche erfahren.

Metadaten sind Informationen über Daten/Dateien. Entsprechend enthalten Foto-Metadaten weitere Informationen zu einem Foto. Sie helfen Fotos zu strukturieren, zu suchen und den Kontext eines Bildes zu bewahren. Sie können zum Beispiel die Zeit eines Fotos speichern oder technische Informationen zur Kamera, jedoch auch den Ort der Aufnahme oder weitere Informationen über das Motiv beinhalten. Metadaten sind oft in den Dateien selbst gespeichert.
Im Rahmen dieser Studie wollen wir nun eine neue Funktion vom Webbrowser Chrome untersuchen. Sie soll Nutzer beim Schutz der eigenen Privatsphäre unterstützen. Nutzt ihr sonst einen anderen Browser, ist das nicht schlimm.

Folgende neue Funktionen untersuchen wir:

1. Beim Surfen geben kleine Icons Hinweise auf Metadaten in Bildern. Ein Klick auf sie zeigt Details.
   - Ein „Rechtsklick auf ein Bild → Zeige Metadaten“ tut dies auch.
2. Beim Hochladen von Bildern mit Metadaten gibt es die Möglichkeit, solche Informationen zu verändern oder zu löschen.
   - Dazu wird das Hochladen unterbrochen und man kann die einzelnen Informationen bearbeiten, löschen und eine Erklärung der Daten lesen.
     → zum Schluss „**Hochladen fortsetzen**“ nicht vergessen

WICHTIG:
In jedem Teil der praktischen Aufgaben gibt es neue Funktionen, die wir untersuchen wollen. Ihr könnt und sollt diese im Folgenden frei verwenden, so wie ihr sie auch zuhause verwenden würdet. Wir ermutigen euch aber auch dazu, vielleicht mehr auszuprobieren. Seht die verwendeten Bilder als eure an und die abgebildeten Personen als eure Freunde oder Bekannte.

Ihr könnt nun selbstständig beginnen.
Dazu einfach der Beschreibung auf dem Bogen *(1) Aufgabenbeschreibung* folgen.

C.3.3 Aufgabenbeschreibung

Willkommen
Damit wir später deine Antworten aus der Terminumfrage korrekt einarbeiten können, gehe nun bitte sicher, dass du am richtigen Platz sitzt. Kontrolliere dazu die auf deinem Fragebogen notierte E-Mail-Adresse.

Du kannst nun selbstständig beginnen.

Bei Fragen gib einfach kurz ein Zeichen und jemand kommt. Lass bitte die anderen neben dir in Ruhe weiterarbeiten.

Teil 1: Intro

- Beantworte **Frage 1 + 2 → auf dem Fragebogen**.

Teil 2: Hochladen von Bildern

Hinweis: Die im Folgenden beschriebenen Dateien findest du auf dem *Windows Desktop* → im Verzeichnis *Bilder*.

- Öffne Chrome.
- Gehe auf die Webseite `https://xyz.dcsec.uni-hannover.de/studie1/`.
- Lade dort das Bild **pinguin.jpg** hoch.
- Hast du uns ein Bild geschickt / hochgeladen?

  JA: Lade **dein Bild** hoch. Es liegt in *Desktop* → *Eigene*.

  NEIN: Lade **ersatzweise** ein Bild hoch: Wähle wenn möglich, deine Telefon-Art, sonst zufällig:

  (a) **Android-Foto_Rezept_Jan.jpg**
  oder (b) **iPhone-Foto_mein_Kollege.jpg**.

- Beantworte **Frage 3 – 5**.
- Lade nun folgende drei Bilder jeweils einzeln hoch[1]:
  1. **Uni-Mobil.jpg**
  2. **CandlelightDinner.jpg**
  3. **Party_11_2.jpg**
- Beantworte **Frage 6 – 11**.

Teil 3: Surfen

- Gehe auf die Webseite `https://xyz.dcsec.uni-hannover.de/studie2/`.
  Diese Seite zeigt ein paar frei zugängliche Bilder im Web. Schaue Dir an, was in den Bildern an Metadaten gespeichert ist. Du kannst über die Links auch die Originalseiten sehen. Surf sie gerne kurz an oder schaue eine der unten verlinkten Fotoseiten und Metadaten dort an.
- Beantworte **Frage 12 – 18**.

[1] Reihenfolge für jede teilnehmende Person gemäß Lateinischem Quadrat angepasst.

Teil 4: Mehr Privatsphäre

- Gehe auf die Webseite `https://xyz.dcsec.uni-hannover.de/studie3/`.
- **Lade** dein beim Hochladen gewähltes Bild hier nochmal **hoch**.
  Erinnerungshilfe: Antwort Frage 3

  Falls notwendig, dein Passwort für den Verschlüsselungsdienst ist:

  studie
- Beantworte **Frage 19 – 20**.

Teil 5: Abschluss

- Beantworte **Frage 21 – 22**.
- Bitte schließe alle Fenster des Chrome-Browsers.

Vielen Dank für deine Teilnahme.
Du kannst nun leise nach vorn kommen. Bringe deine Zettel bitte mit.
Nach einer Quittungsunterschrift erhältst du deine Aufwandsentschädigung.

C.3.4 Papier-Fragebogen

Zur Studie – zum Nachlesen – wurde schon vorgetragen

Im Rahmen dieser Studie wollen wir eine neue Funktion vom Webbrowser Chrome untersuchen. Sie soll Nutzer wie dich beim Schutz der eigenen Privatsphäre unterstützen.

Neue Funktionen:

- Beim Surfen geben dir kleine Icons hinweise auf Metadaten in Bildern. Ein Klick auf sie zeigt dir Details.
  - „Rechtsklick auf ein Bild → Zeige Metadaten“ tut dies auch.
- Beim Hochladen von Bildern mit Metadaten hast du die Möglichkeit, solche Informationen zu verändern oder zu löschen.
  - Das Hochladen wird unterbrochen und du kannst die einzelnen Informationen bearbeiten, löschen und eine Erklärung der Daten lesen. Gehe mit dem Mauszeiger über eine Information und die entsprechenden Icons erscheinen.
    → zum Schluss „Hochladen fortsetzen“ klicken.

In jedem Teil der praktischen Aufgaben gibt es neue Funktionen. Du kannst und sollst diese im Folgenden frei verwenden, so wie du sie auch zuhause verwenden würdest.

Intro

1. Inwieweit machst du dir Gedanken darüber, ob/wo/wie du im Netz persönliche Informationen preisgibst?

	gar nicht				sehr viel / häufig
Gedanken machen	○0	○4	○6	○21	○12

2. Schätze ein, wie sehr du die Kontrolle darüber hast, was du von Dir preisgibst, wenn du Fotos im Netz teilst.

	gar nicht				voll und ganz
Kontrolle haben	○4	○18	○12	○6	○3

Hochladen von Bildern

3. Dateinamen des eigenen/gewählten Bildes bitte eintragen:
Eindeutiger Anfang des Namens reicht aus.

4. Inwieweit hast du (auf Anhieb) verstanden, was Dir – jetzt neu – beim Hochladen der Bilder angezeigt wird?

	gar nicht				voll und ganz
verstanden	○2	○4	○8	○16	○13

5. Wusstest du, dass solche Informationen in (deinen) Bildern gespeichert sind?

10○ ja
25○ teils; ich wusste, dass Informationen drin sind, aber nicht genau welche
8○ nein

Hochladen von Bildern – fortgesetzt

6. Wie findest du die Integration des Bearbeitens/Löschens direkt beim Hochladen von Fotos?

	hinderlich / unpraktisch / nervig				äußerst praktisch / sehr gut
Zeigen+Bearbeiten-Dialog	○1	○1	○6	○10	○25

7. Wie häufig würdest du die neuen Funktionen auch in deinem Browser zuhause nutzen wollen?

	nie		ab und zu		immer
zeigen/ansehen	○2	○0	○9	○8	○24
verändern	○2	○5	○9	○15	○12
löschen	○1	○1	○14	○7	○20

8. Inwieweit verbessert diese Erweiterung dein Wissen darüber, was du mit deinen Fotos zusammen teilst?

	gar nicht				sehr stark
Bewusstsein	○1	○2	○1	○10	○29

9. Inwieweit verbessert diese Erweiterung deine Kontrolle darüber, was du mit deinen Fotos zusammen teilst?

	gar nicht				sehr stark
Kontrolle	○1	○1	○4	○14	○23

10. Fehlt Dir eine Funktion, die du noch gerne nutzen würdest?

7○ ja
20○ nein
16○ weiß nicht

Bitte schreibe einen Kommentar zu deiner Auswahl:

11. Bitte bewerte die folgenden Aussagen zu der gerade verwendeten neuen Funktion (Pop-up, Metadaten sehen / ändern / löschen):

	trifft nicht zu				trifft voll zu
Ich glaube, dass ich diese neue Funktion gerne oft benutzen würde.	○2	○1	○3	○14	○23
Ich fand die neue Funktion unnötig komplex.	○24	○11	○5	○2	○1
Ich denke, dass die neue Funktion einfach zu benutzen war.	○1	○3	○6	○14	○19
Ich fand, dass die neue Funktion gut integriert war.	○1	○2	○4	○15	○21
Ich fand die Funktion zu inkonsistent.	○13	○19	○10	○1	○0
Ich fand, dass die neue Funktion sehr mühsam zu benutzen war.	○19	○16	○4	○2	○2
Ich bin mir sicher, die neue Funktion richtig benutzt zu haben.	○2	○1	○9	○15	○16
Ich denke, ich bräuchte technische Unterstützung von einer anderen Person, um die neue Funktion zu benutzen.	○22	○14	○4	○2	○1
Ich denke, dass die meisten Leute sehr schnell lernen würden, mit der neuen Funktion umzugehen.	○2	○2	○7	○15	○17
Ich musste erst viel lernen, bevor ich mit dieser neuen Funktion loslegen konnte.	○32	○4	○5	○1	○1

Surfen

12. Wie hilfreich sind für dich die Hinweis-Icons auf den Bildern für die Übersicht, was für private Informationen in den Bildern sind?

	gar nicht hilfreich				äußerst hilfreich
Icons hilfreich?	○1	○3	○7	○12	○20

13. Wie stark stören dich die Hinweis-Icons auf den Bildern beim Surfen?

	stören gar nicht				stören sehr
Icons störend?	○27	○12	○3	○1	○0

14. Wie empfindest du die Darstellung in der Detailansicht?

	Unnütz / ablenkend / unpassend		neutral		sehr hilfreich
Gruppierung (Ort, Personen, Inhalt, ...)	○1	○0	○7	○21	○14
rot hinterlegt = sehr privat	○0	○4	○9	○10	○20
Karte für Koordinaten	○2	○1	○6	○16	○18
Personen-Markierungen in kleinem Bild	○1	○3	○10	○16	○13
Erklärungen beim mit Maus Darüberschweben	○2	○6	○8	○11	○16
Ansicht aller Informationen möglich	○1	○2	○9	○11	○20

15. Hättest du gerne noch mehr Unterstützung dabei zu entscheiden, was deine Privatsphäre bedrohen könnte?

	gar nicht				auf jeden Fall
mehr Hilfe	○1	○5	○3	○14	○20

16. Inwieweit hilft Dir diese neue Funktion einen besseren Überblick / ein besseres Bewusstsein zu haben, was alles noch in Bildern gespeichert ist, die <u>du und andere</u> im Netz teilen?

	hilft gar nicht				hilft sehr gut
Schafft Bewusstsein?	○1	○0	○1	○10	○31

17. Wie häufig würdest du diese neuen Funktionen auch in deinem Browser zuhause nutzen wollen?

	nie		ab und zu		immer
Hinweis-Icons	○0	○1	○10	○13	○19
Details ansehen	○0	○4	○11	○14	○14

18. Bitte bewerte die folgenden Aussagen zu der gerade verwendeten neuen Funktion (Hinweis-Icons, Detailansicht mit Gruppierung der Informationen, farbige Markierung usw.):

	trifft nicht zu				trifft voll zu
Ich glaube, dass ich diese neue Funktion gerne oft benutzen würde.	○1	○1	○2	○20	○19
Ich fand die neue Funktion unnötig komplex.	○24	○10	○8	○1	○0
Ich denke, dass die neue Funktion einfach zu benutzen war.	○0	○2	○3	○13	○25
Ich fand, dass die neue Funktion gut integriert war.	○1	○1	○3	○19	○19
Ich fand die Funktion zu inkonsistent.	○20	○11	○12	○0	○0
Ich fand, dass die neue Funktion sehr mühsam zu benutzen war.	○24	○15	○3	○0	○1
Ich bin mir sicher, die neue Funktion richtig benutzt zu haben.	○1	○3	○1	○22	○16
Ich denke, ich bräuchte technische Unterstützung von einer anderen Person, um die neue Funktion zu benutzen.	○29	○10	○3	○1	○0
Ich denke, dass die meisten Leute sehr schnell lernen würden, mit der neuen Funktion umzugehen.	○1	○1	○5	○21	○15
Ich musste erst viel lernen, bevor ich mit dieser neuen Funktion loslegen konnte.	○34	○6	○3	○0	○0

Mehr Privatsphäre

19. Siehst du die Zusatzinformationen in den Bildern eher als Bedrohung für deine Privatsphäre an oder siehst du die Informationen auch als sinnvoll an (z. B. zum Ordnen, Suchen oder besser Erinnern)?

	Bedrohung der Privatsphäre			nützlich & sinnvoll	
beim Hochladen & Teilen	○26	○7	○7	○3	○0
beim Teilen mit Einzelnen (z. B. via E-Mail)	○1	○4	○6	○21	○11
privat/offline	○2	○0	○1	○8	○32

20. Was würdest du bevorzugen, um Metadaten beim Teilen zu schützen?

Bitte nummeriere jede Box in der Reihenfolge deiner Präferenz, beginnend von 1 bis 4

1×1, 2×2 3×3,37×4	lassen wie sie sind
11×1,23×2 8×3, 1×4	selektiv löschen / bearbeiten
17×1, 8×2 16×3, 2×4	immer alles löschen
14×1,10×2 16×3, 3×4	verschlüsseln, um Zugriff einzuschränken

Abschluss

21. Hast du durch die neuen Funktionen des Browsers etwas dazu gelernt oder wahrgenommen, wodurch sich deiner Meinung nach etwas an deiner Meinung, Einstellung, Verhalten ändern könnte?

5○ nein
38○ ja

Bitte schreibe einen Kommentar zu deiner Auswahl:

Machst du dir mehr Gedanken?
Schätzt du deine Kontrolle anders ein?
Meinst du diese Neuerung wird Dir helfen?

22. Hast du zu Beginn beim Hochladen (*studie1*) Metadaten bearbeitet oder gelöscht? Bitte erläutere in mindestens einem Satz wieso beziehungsweise wieso nicht.

25○ nein
18○ ja

Bitte schreibe einen Kommentar zu deiner Auswahl:

C.3.5 Verwendete Bilder

Im Folgenden werden die innerhalb der Laborstudie verwendeten Bilder beschrieben. Auch wenn es sich bei den Bildern um Beispiele im Web öffentlich zugänglicher Bilder handelte, werden diese hier nicht abgedruckt.

Die im Folgenden angegebenen Metadaten wurden zum Schutz der betroffenen Personen zum Teil verfälscht. Die Art und Granularität der enthaltenen Daten kann jedoch weiterhin eingeschätzt werden.

Hochladen von Bildern

Pinguin Foto eines tauchenden Pinguins. Das Foto enthielt keine Metadaten. Es wurde folglich von der Browser-Erweiterung ignoriert, da keine Informationen zum Anzeigen oder Verändern vorhanden waren.

iPhone-Foto_mein_Kollege Foto eines Mitarbeiters der Arbeitsgruppe Distributed Computing & Security an seinem Schreibtisch. Das Gesicht der Person war geschwärzt. Metadaten waren unverändert, wie sie ein iPhone 5 im Bild speichert.

Personen-Markierung:	Gesicht der Person markiert; kein Name gespeichert
Vorschaubild:	Gesicht nicht geschwärzt
GPS-Koordinaten:	N 52° 22' 45.372" E 9° 43' 21.9"
Datum / Zeit:	10.10.2013 11:32:08
Kameramodell:	iPhone 5
Software:	7.0.2

Android-Foto_Rezept_Jan Foto eines handschriftlich notierten Rezeptes. Metadaten waren unverändert wie sie ein Smartphone vom Modell HTC Desire im Bild speichert.

GPS-Koordinaten:	N 52° 21' 37.69" E 9° 45' 31.14"
GPS-Datum:	31.08.2013
GPS-Zeit:	18:13:11
Kameramodell:	HTC Desire

Party_11_2 Foto einer Gruppe von sechs Studierenden bei einer Party des Hochschulsports. Gesichter waren deutlich zu erkennen.

Personen-Markierung:	Gesicht einer Person markiert; Name: Saskia Krüger
Titel:	Show & Snow Party
Datum / Zeit:	14.10.2013 22:41:02
Software:	Picasa

Uni-Mobil Nahaufnahme eines wertvollen Fahrrads am Fahrradständer vor dem Hauptgebäude der Leibniz Universität Hannover.

Ersteller:	Moe Falk
Kameraseriennummer:	1007090509
GPS-Datum:	07.10.2013
Datum / Zeit:	07.10.2013 16:19:57
Kameramodell:	EOS 450D

CandlelightDinner Foto eines vorbereiteten Tisches für ein gemütliches Abendessen bei Kerzenlicht.

GPS-Koordinaten:	N 52° 23' 2.904" E 9° 43' 24.888"

Surfen

DCSec-Gruppenbild Gruppenfoto der Arbeitsgruppe Distributed Computing & Security wie es auf der Webseite der Gruppe zu finden war.

Ersteller:	Benjamin Henne
Kameraseriennummer:	12345678
GPS-Koordinaten:	N 52° 22' 50.124" E 9° 43' 10.56"
Datum / Zeit:	18.07.2011 11:19:26
Kameramodell:	EOS 60D

Flickr: Kind Foto eines Kindes, welches ein selbst gemaltes Bild in die Kamera hält.

Personen-Markierung:	Gesicht des Kindes markiert; Name: Joel Johnson
Kamerabesitzer:	Oliver Johnson
Kameraseriennummer:	404382837
Kameramodell:	Canon EOS DIGITAL REBEL
Software:	Picasa

Flickr: Vater mit Kindern Ein asiatischer junger Vater mit zwei kleinen Kindern auf dem Arm im Flur einer Wohnung.

GPS-Koordinaten:	N 36° 20' 10.32" E 127° 22' 49.08"
Kompassrichtung:	79.5°
Datum / Zeit:	04.02.2012 11:14:28
Kameramodell:	iPhone 4

Flickr: Spiegelpose ohne Kopf Ein junges Mädchen fotografiert sich selbst posierend in Hotpants und Bluse vor einem Spiegel. Das Bild war beschnitten, so dass der Kopf nicht zu sehen war.

Vorschaubild:	Mädchen inklusive Kopf erkennbar abgebildet
Datum / Zeit:	19.07.2012 11:17:53
Kameramodell:	iPhone 3GS
Software:	MS Windows Photo Gallery

C.3.6 Protokollierung von Nutzeraktionen

Um alle Aktionen der Teilnehmer später analysieren zu können, wurde die Browser-Erweiterung für die Laborstudie so erweitert, dass alle Nutzeraktionen über einen zentralen Webservice protokolliert wurden. Listing C.1 zeigt exemplarisch eine gefilterte, strukturierte Darstellung eines protokollierten Studiendurchlaufs ohne die Zeitstempel der einzelnen Einträge.

Listing C.1: Protokollierte Aktionen eines Laborstudienteilnehmers

```
surveyID=98 PC=kpc1 start=2013-10-18 09:30:00 end=2013-10-18 10:04:00
  visit /studie1
    no_metadata
      uploaded /studie1 f0ee[...]04a4+pinguin.jpg
    viewing details Uni-Mobil.jpg
      delete metadata Exif.GPSInfo.GPSDateStamp
      delete metadata Iptc.Application2.Byline
      delete metadata Exif.Photo.BodySerialNumber
      uploaded /studie1 f0ee[...]04a4+Uni-Mobil.jpg
    viewing details Party_11_2.jpg
      delete metadata Xmp.mwg-rs.Regions/mwg-rs:RegionList[1]/mwg-rs:Name
      uploaded /studie1 f0ee[...]04a4+Party_11_2.jpg
    viewing details CandlelightDinner.jpg
      delete metadata ALL
      uploaded /studie1 f0ee[...]04a4+CandlelightDinner.jpg
  visit /studie2
    open http://www.dcsec.uni-hannover.de/
      viewing details dcsec_group_2011_m.jpg
    open http://www.flickr.com/photos/xxxxxx/7183354611/in/photostream/
      viewing details 71xxxxxx11_2xxxxcdc9f_o.jpg
    revisit /studie2
      viewing details 75xxxxxx26_bxxxx32884_o.jpg
      viewing details 73xxxxxx00_3xxxxf3c29_o.jpg
      viewing details 75xxxxxx26_bxxxx32884_o.jpg
      viewing details 71xxxxxx11_2xxxxcdc9f_o.jpg
      viewing details 75xxxxxx26_bxxxx32884_o.jpg
      viewing details 71xxxxxx11_2xxxxcdc9f_o.jpg
      viewing details dcsec_group_2011_m.jpg
      viewing details 75xxxxxx26_bxxxx32884_o.jpg
    open http://www.flickr.com/photos/xxxxxxxx@N04/7508248026/in/photostream/
    open http://www.flickr.com/photos/xxxxxxxx@N04/7383706800/
    open http://www.fotocommunity.de/galerie
    open http://www.flickr.com/search/?q=recent&cm=apple/iphone_4s
  visit /studie3
    viewing details iPhone-Foto_mein_Kollege.jpg
      share metadata audience 2
      caas password studie
      uploaded /studie3 f0ee[...]04a4+iPhone-Foto_mein_Kollege.jpg
    viewing details studie3:f0ee[...]04a4 iPhone-Foto_mein_Kollege.jpg
```

C.4 Fokusgruppen zur Nutzung und zum Schutz von Standortinformationen

In diesem Abschnitt werden Materialien der durchgeführten Fokusgruppen für ein besseres Verständnis bereitgestellt.

C.4.1 Zielbeschreibung

Die Zielbeschreibung der Studie:
Apps auf mobilen Geräten ermöglichen Nutzern eine Vielzahl an Dingen zu tun. Außer für E-Mail, Internet und als Kamera dienen Smartphones beispielsweise als Navigationsgerät und als Spielkonsole. Apps erleichtern ihren Nutzern den Alltag, indem sie spezialisiert den Zugriff auf Informationen oder Internetdienste wie auch Soziale Onlinenetzwerke vereinfachen. Eine Vielzahl der Apps verwendet dabei private Nutzerdaten. Ein Teil tut dies zur Verbesserung der gebotenen Funktionalität, während andere Apps bzw. dahinter liegende (Werbe-)Anbieter darauf aus sind, Daten zu sammeln oder Nutzer beispielsweise zu Werbezwecken zu identifizieren, zu klassifizieren und zu lokalisieren. Bisher war der Fokus der Forschung im Bereich IT-Sicherheit auf das Identifizieren und Verhindern von Datenklau gerichtet. Es existieren jedoch auch viele Apps bei denen die Nutzer private Daten wie beispielsweise (und hier speziell) ihren Aufenthaltsort verwenden wollen – Apps auf einer breiten Skala von Navigations-Apps bis zur Wettervorhersage des aktuellen Orts. Viele dieser Apps benötigen jedoch nicht den genauen Ort einer Person. Somit liegt es nahe, die Privatsphäre der Personen zu schützen, indem man die Daten nur so genau wie für den jeweiligen Anwendungsfall notwendig an die jeweilige App herausgibt. Aus dieser Grundannahme entstehen die folgende Fragen.

Leit- und Zielfragen

- Sind sich die Nutzer ihrer Situation bewusst?
  - Welche Apps nutzen ihren Ort?
  - Welche Apps brauchen ihren Ort?
  - Welche Genauigkeit braucht eine App, um zu funktionieren?
- Was wünschen sich die Nutzer?
  - Mehr Kontrolle?
  - Selbst reglementieren oder Kontrollmöglichkeit aber regeln lassen
  - Ein pragmatisches Ergebnis oder konzeptionell anspruchsvolle Algorithmen?
- Womit haben Nutzer Schwierigkeiten?
  - Algorithmen-Konzepte?
  - Parameter-Verständnis?
  - Parameterwerte-Wahl?
  - App-Abhängigkeit der Parameter?

C.4.2 Online-Fragebogen zur Teilnehmer-Rekrutierung

Folgende Informationen wurden von den potenziellen Teilnehmern für die Gruppenbildung und Terminplanung gesammelt.

1. Mögliche Teilnahme an vorbestimmten Terminen
2. E-Mail-Adresse für weitere Benachrichtigungen
3. Alter
4. Studienrichtung
5. Erlaubnis zur Tonaufzeichnung bei einer Teilnahme
6. Selbsteinschätzung der technischen Expertise: 5-Punkte-Skala von *(1) Ich nehme oft Hilfe in Anspruch* bis *(5) Ich helfe oft Anderen*
7. Privacy Segmentation nach Westin
8. Informationen zu verwendeten Apps

   Antworten: *(1) kenne ich nicht / (2) nutze ich nicht / (3) wenige male genutzt / (4) nutze ich je Woche / (5) nutze ich täglich/ (6) nutze mehrmals täglich*

   App-Typen: Browser, Mail, Kalender / Kamera / Spiele / werbefinanzierte Apps / [ich lese] Soziale Netzwerke (wie Facebook, Instagram, Twitter) / [ich poste] Soziale Netzwerke / Karten, Navigation, Geocaching / Wetter, Nachrichten / Auskünfte (wie Gelbe Seiten, Qype, Yelp, Google Local, mehr-tanken) / Musik, Internetradio (z. B. Shazam, AUPEO!, Tuneln) / Fahrplanauskunft, Lieferdienst / Location-Sharing (wie Google Latitude, Foursquare)
9. Informationen zu verwendeten mobilen Geräten
   Antworten: *besitze ich nicht / niemals / seltener als wöchentlich / wöchentlich / mehrmals wöchentlich / täglich / mehrmals täglich*

   Geräte-Typen: Android Smartphone / Windows Smartphone / Apple iPhone / Anderes Smartphone / Android Tablet / Windows Tablet / Apple iPad / anderes Tablet / sonstiges mobiles Gerät (Smartwatch, . . .)
10. Verwendete Technologien

    Antworten: *kenne ich nicht / nie / hin und wieder / häufig / weiß nicht, ob ich es vielleicht unbewusst nutze*
    Technologien: Bluetooth / WLAN / GPS / NFC

C.4.3 Teilnehmer der Fokusgruppen

Tabelle C.1 zeigt die Zusammensetzung der drei Fokusgruppen.

Tabelle C.1: Teilnehmer der drei Fokusgruppen

Demographie

Lfd. Nr.	Gruppe	Alter	Geschlecht	Studienrichtung	technische Expertise	Westin	eigenes Gerät	verwend. Apps ø
1	1	19	m	Chemie	4	Funda	Android	4
2	1	22	w	Life Science	3	Fund	Android	4
3	1	25	w	Maschinenbau	3	Pragm	Apple	4
4	1	24	w	Pädagogik	3	Fund	Android	5
5	1	24	w	Pflanzenbiotechnologie	2	Fund	Android	4
6	1	20	m	Politikwissenschaften	4	Pragm	Apple	4
7	1	23	m	Wirtschaftsingenieurwesen	5	Pragm	Apple	4
8	2	23	m	Jura	3	Fund	Apple	4
9	2	24	m	Maschinenbau	5	Fund	Android	5
10	2	28	m	Pädagogik	5	Pragm	Android	5
11	2	44	w	Pädagogik	3	Fund	Apple	6
12	2	20	w	Pflanzenbiotechnologie	3	Fund	Apple	5
13	2	26	m	Physik	4	Pragm	Android	5
14	2	22	w	Wirtschaftsingenieurwesen	3	Pragm	Android	4
15	3	22	w	Englisch	2	Fund	Android	4
16	3	25	w	Geographie	3	Pragm	Android	5
17	3	24	w	Lebensmittelwissenschaften	2	Pragm	Apple	5
18	3	25	m	Maschinenbau	5	Pragm	Android	4
19	3	29	m	Maschinenbau	4	Fund	Android	5
20	3	23	w	Pädagogik	3	Pragm	Android	4

verwendete Apps

Lfd. Nr.	PIM	Kamera	Spiele	Werbe-finanz.	lese in SN	poste in SN	Navi	Wetter	Auskunft	Musik	Fahrplan	Ort teilen
1	6	4	6	5	6	3	2	3	4	3	4	2
2	6	4	2	5	6	2	5	6	3	5	4	2
3	6	4	6	1	2	2	4	5	3	4	4	4
4	6	6	4	5	6	4	5	6	5	6	6	2
5	5	3	4	6	3	3	6	6	6	3	3	2
6	6	4	4	4	6	4	4	5	3	4	4	2
7	5	5	3	4	5	4	4	5	5	6	3	2
8	5	4	5	4	3	3	4	6	4	3	4	2
9	6	5	6	5	6	6	4	6	3	4	5	1
10	6	6	3	4	6	5	4	5	4	3	5	4
11	6	6	6	5	6	6	6	6	6	5	3	4
12	6	4	4	6	6	4	4	6	4	3	4	3
13	6	5	6	6	6	3	4	6	3	6	4	2
14	6	4	3	3	6	3	3	5	6	2	4	1
15	2	5	3	4	6	2	5	5	6	2	4	2
16	6	4	6	4	6	4	4	4	6	3	5	2
17	6	6	6	2	4	4	4	5	5	5	6	4
18	6	4	3	3	6	3	4	6	4	5	6	2
19	5	4	6	5	6	5	3	6	4	5	5	4
20	6	3	4	6	6	5	4	6	3	2	5	4

C.4.4 Frageplan

Folgender Fragenplan wurde in den Fokusgruppen verwendet. Zwei der drei Gesprächsrunden verliefen so selbstständig, dass sie von allein gemäß des hier skizzierten roten Fadens abliefen. Die dritte bedurfte geringfügiger Steuerung.

Begrüßung [Ausschnitte]

Danke, dass ihr euch die Zeit genommen habt, an unserer Gruppendiskussion zur Nutzung von Apps auf mobilen Geräten teilzunehmen.

Wir arbeiten in der Forschung derzeit daran, besser zu verstehen, wie Nutzer Apps auf mobilen Geräten im Alltag verwenden und welches Bewusstsein und Verständnis sie über die Funktion von Apps besitzen. Durch unsere Untersuchungen hoffen wir, bessere und sichere Lösungen für App-Nutzer zu finden. Heute möchten wir gerne eure Ansichten zu Apps hören, mit denen ihr entweder Informationen im Netz postet oder ihr aktuelle Informationen aus dem Netz abruft.

Ihr wurdet eingeladen, da ihr als Teil einer besonders mobilen Generation entsprechende mobile Geräte noch offener und alltäglicher nutzt als Andere. Als Studenten seid ihr zudem Teil der Gruppe von Menschen, die sich häufiger kritische Gedanken über Dinge machen. Wir möchten gerne von eurem Erfahrungsschatz profitieren.

Wir diskutieren heute über mobile Geräte. Alle von euch haben entweder ein iPhone oder ein Android-Telefon und teilweise auch mehrere mobile Geräte. Wenn wir diskutieren, sollten wir alle im Kopf behalten, dass es zumindest kleine Unterschiede gibt, wie Apple iOS und Android manches umsetzen. Die Diskussion sollte jedoch eigentlich so herstellerunabhängig ablaufen, dass es nicht groß auffällt.

Es gibt keine falschen oder richtigen Antworten. Wir gehen fest davon aus, dass ihr unterschiedlicher Meinung sein werdet, und möchten euch daher auch bitten, widersprüchliche Ansichten zum Ausdruck zu bringen, auch wenn es sich von dem unterscheidet, was andere gesagt haben. Wir zeichnen daher die Diskussion auch auf, weil wir keinen eurer Kommentare verpassen möchten. Wir werden natürlich alle Daten nur anonymisiert auswerten und die Aufzeichnung später vernichten.

Opening

1. Zur Vorstellung nennt bitte nochmal euren Namen und welche mobilen Geräte ihr wie häufig im Alltag nutzt.

Introductory

2. Welche Art von Apps und welche Funktionen nutzt ihr am liebsten und am meisten, wenn ihr unterwegs seid?

Transition

Im Weiteren dieser Diskussionsrunde wollen wir uns heute auf Apps fokussieren, die den aktuellen Aufenthaltsort von Nutzern verwenden. Häufig spricht man hier auch von standortbezogenen Apps.

3. Habt ihr die Verwendung eures aktuellen Standortes auf euren Telefonen angeschaltet oder ausgeschaltet? Was hat euch dazu veranlasst es so einzustellen?
4. Wozu verwendet ihr Apps, die euren aktuellen Aufenthaltsort verwenden?

5. Welche Gedanken macht ihr euch darüber, ob und welche Apps euren aktuellen Aufenthaltsort nutzen, um euch die versprochenen Funktionen zu bieten?
6. Habt ihr schon einmal eine App nicht installiert oder nicht genutzt und wieder deinstalliert, weil sie euren aktuellen Standort verwendet, den ihr der App oder einem Anbieter dahinter nicht geben wollt?
    - Wenn ja, könnt ihr uns anderen kurz erläutern wieso.
7. Könnt ihr uns sagen, wie man herausfinden kann, ob eine App den aktuellen Aufenthaltsort verwendet?

Key

Für alle verbreiteten mobilen Geräte gibt es eine Menge von Apps, die den aktuellen Standort des Nutzers verwenden. Je nach Betriebssystem kann man die Verwendung des aktuellen Ortes komplett für alle Apps ausschalten oder sogar für einzelne Apps. Hier unterscheiden sich Apple und Android: Beim iPhone und iPad kann man die Verwendung von Ortsinformationen für alle Apps verbieten oder aber für jede Einzelne an- und ausschalten. Bei Android gibt es nur den An-Aus-Schalter für alle Apps auf einmal.

8. Wünscht ihr euch eine bessere Einstellmöglichkeit für die Verwendung von Ortsinformationen, d. h. mehr Kontrolle?
    - Was genau für Einstellmöglichkeiten würdet ihr euch wünschen?
    - Auf welche Art und Weise würde das eure Nutzung solcher Apps verändern?
9. Bisher kann man wie gesagt auf den Geräten für alle Apps auf einmal oder eben pro App das Verwenden des aktuellen Ortes unterbinden. Dies ermöglicht einem zum Beispiel bei einer App – speziell oft auch bei Spielen oder Demoversionen – die Verwendung zu unterbinden, wenn man sich selbst nicht sicher ist, wozu die App den Ort braucht.
    - Woran macht ihr fest, welche Apps den Ort wirklich brauchen? Schaut gerne kurz auf eure Telefone, wenn euch das hilft.
    - Wie sicher seid ihr euch dabei, dass ihr die richtigen Entscheidungen trefft?
10. Neben vielen Apps bei denen infrage steht, ob sie den Ort wirklich benötigen, gibt es auch verschiedene Apps, die den Ort benötigen bzw. wo ihr den Ort verwenden wollt. Ein Beispiel: Ihr seid in einer fremden Kleinstadt, sagen wir Goslar, und ihr sucht ein schönes Café oder ein Restaurant in der Stadt.
    - Welche Möglichkeiten fallen euch ein, um nach diesen zu suchen und dabei möglichst wenig dem Suchdienst-Anbieter gegenüber preiszugeben?
11. Eine technische Möglichkeit wäre, dass man einstellen könnte, dass der Suchdienst nur erfährt, in welcher Stadt ihr euch gerade befindet, da er für die Suche ja nicht wissen muss, an welcher Straßenecke ihr gerade euer Telefon benutzt.
    - In wie weit fühlt ihr euch in der Lage zu beurteilen, welche Genauigkeit eine App braucht, damit sie einerseits funktioniert und ihr das bekommt, was sie euch bieten soll und andererseits auch nur das verratet, was sein muss?

12. Wir können dies mal an zwei kurzen Beispielen gemeinsam in der Runde überlegen. Als Anregung liegt vor euch eine Liste mit verschiedenen App-Kategorien, von denen zumindest die bekanntesten Ortsinformationen verwenden, um gewisse Features anzubieten. Gerne könnt ihr auch eine App von eurem Telefon nehmen, wenn ihr da einen schwierigen Fall seht. Wer möchte mal eine Einschätzung vorgeben, die wir dann diskutieren können?
13. Schätzt bitte mal ein, ob ihr euch zutraut, die Einstellungen für Apps, die ihr auf eurem Telefon nutzt zu treffen? Schaut ruhig auf eure Telefone.
14. Welchen Anbietern oder Personen würdet ihr solch eine Entscheidung sonst zutrauen und entsprechend auf euren Geräten verwenden (=vertrauen)?

Optional, abhängig von der Gruppe

15. Es gibt in der Forschung viele Vorschläge dazu, wie man solch eine sogenannte Verschleierung des Ortes erreichen kann. Es gibt einfache Ansätze, wie das Runden von Koordinaten oder das Verschieben des wahren Standortes um x Meter in eine zufällige Richtung. Ebenso gibt es Ansätze, die einem Nutzer zum Beispiel versprechen, man sei unter x anderen Personen nicht zu erkennen, die also den Ort so ungenau machen, dass die Ortsangabe auf mindestens so viele Personen passt, die eine App nutzen.
    Geht davon aus, dass eure Telefone und Tablet können eure Koordinaten ungenau machen. Worauf käme es euch dabei an?

    - minimale/maximale Ungenauigkeit, vorstellbar, gute Methoden

16. Da wir noch etwas Zeit haben, geben wir euch einen Zettel aus, auf dem ein paar verschiedene Verfahren skizziert sind. Schaut sie euch kurz an. Gibt es da etwas, was ihr besonders gut oder besonders schlecht findet?

Abbildungsverzeichnis

Tabellenverzeichnis

Verzeichnis der Listings

Literaturverzeichnis

Webquellen

[1] ARD/ZDF: *ARD/ZDF-Onlinestudie 2013*. http://www.ard-zdf-onlinestudie.de/, September 2013

[2] Bild.de (Rickmann, A.): *So viele Fotos posten die eigenen Freunde wirklich*. http://www.bild.de/digital/internet/facebook/app-zaehlt-fotos-der-freunde-auf-facebook-31200354.bild.html, Juli 2013

[3] BITKOM: *Consumer Electronics 2013: Marktentwicklung und Trends*. http://www.bitkom.org/files/documents/BITKOM_Praesentation_CE-PK_02_09_2013.pdf, September 2013

[4] ComScore MobiLens: *Anteil Smartphone-Nutzer an Mobiltelefonbesitzern*. http://de.statista.com/statistik/daten/studie/237079/umfrage/anteil-der-smartphone-nutzer-an-allen-mobilfunknutzern-in-deutschland/, Oktober 2013

[5] ComScore MobiLens: *Marktanteile der Betriebssysteme an der Smartphone-Nutzung in den USA von Oktober 2011 bis Oktober 2013*. http://de.statista.com/statistik/daten/studie/77324/umfrage/marktanteile-der-betriebssysteme-fuer-smartphones-in-den-usa/, Dezember 2013

[6] ComScore MobiLens: *Marktanteile der Betriebssysteme an der Smartphone-Nutzung in Deutschland von Dezember 2011 bis September 2013*. http://de.statista.com/statistik/daten/studie/170408/umfrage/marktanteile-der-betriebssysteme-fuer-smartphones-in-deutschland/, November 2013

[7] Controlled Vocabulary, IPTC Photo Metadata Working Group: *Social Media sites: photo metadata test results*. http://www.embeddedmetadata.org/social-media-test-results.php, Juni 2013

[8] CRN.de (Reder, B.): *Versicherung recherchiert auf Facebook nach Blaumachern*. http://www.crn.de/panorama/artikel-8547.html, November 2009

[9] CyanogenMod: *Android Community Operating System*. http://www.cyanogenmod.org/

[10] DRadio Wissen: *Facebook – Pictures of me*. https://web.archive.org/web/20130630120421/http://wissen.dradio.de/facebook-pictures-of-me.36.de.html?dram:article_id=250774, Juni 2013

[11] Exiv2 Projekt (Henne, B.): *Adding new XMP namespaces.* http://dev.exiv2.org/boards/3/topics/1039, Januar 2012

[12] Facebook: *Facebook Reports Fourth Quarter and Full Year 2013 Results.* http://investor.fb.com/releasedetail.cfm?ReleaseID=821954, Januar 2914

[13] FAZ (Gropp, M.): *Facebook erlaubt ein bisschen Anonymität.* http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/der-facebook-boersengang/anonymous-login-facebook-erlaubt-ein-bisschen-anonymitaet-12922752.html, Mai 2014

[14] Forbes.com (Geron, T.): *Viewdle's SocialCamera App Tags And Learns Your Friends' Faces.* http://www.forbes.com/sites/tomiogeron/2011/04/27/viewdles-socialcamera-app-tags-and-learns-your-friends-faces/, April 2011

[15] Forsa/Accenture: *Mobile Web Watch 2013.* http://de.statista.com/statistik/daten/studie/197383/umfrage/mobile-internetnutzung-ueber-handy-in-deutschland/, September 2013

[16] FutureZone (Wimmer, B.): *App von WU-Studenten zeigt, was Facebook über User weiß.* http://futurezone.at/netzpolitik/app-von-wu-studenten-zeigt-was-facebook-ueber-user-weiss/47.822.498, Januar 2014

[17] Github (Henne, B. ; F. Ludwig ; Szongott, C. ; Tute, P.): *Mobile Security & Privacy Simulator.* http://bhenne.github.io/MoSP/, August 2012

[18] Github (Henne, B. ; Protsch, C.): *Mobile Security & Privacy Simulation Geo Tool for OSM map manipulation.* http://bhenne.github.io/MoSP-Geo-Tool/, April 2012

[19] Github (Henne, B. ; Salomon, P. ; C. Szongott): *Mobile Security & Privacy extended Siafu Simulator.* http://bhenne.github.io/MoSP-Siafu/, April 2012

[20] Gizmodo (Biddle, S.): *Vice Magazine Just Accidentally Revealed Where John McAfee Is Hiding.* http://gizmodo.com/5965295/vice-magazine-just-accidentally-revealed-where-john-mcafee-is-hiding, März 2012

[21] Hawk, Thomas: *Is there a major security hole in Flickr's new "geo-fences" feature?* http://thomashawk.com/2011/08/is-there-a-major-security-hole-in-flickrs-new-geo-fences-feature.html, August 2011

[22] Infographic Labs: *Facebook 2012.* http://infographiclabs.com/news/facebook-2012/, Februar 2012

[23] Inside Facecook (Eldon, E.): *New Facebook Statistics Show Big Increase in Content Sharing, Local Business Pages.* http://www.insidefacebook.com/2010/02/15/new-facebook-statistics-show-big-increase-in-content-sharing-local-business-pages/, Februar 2010

[24] Instagram: *Press Page.* http://instagram.com/press/, Dezember 2013

[25] KABC (Romero, R.): *Are insurance companies spying on your Facebook page?* http://abclocal.go.com/kabc/story?id=8422388, November 2011

[26] KISSmetrics: *The History of Photo Sharing.* http://blog.kissmetrics.com/wp-content/uploads/2011/12/photo-sharing.pdf, Dezember 2011

[27] Leibniz Universität Hannover – Referat für Kommunikation und Marketing: *Fotos im Netz: Studie befasst sich mit Bewusstsein über Verwendung von Bildern.* http://www.uni-hannover.de/de/aktuell/presseinformationen/archiv/details/13573/, Juni 2013

[28] Mashable.com (Fox, Z.): *The 10 Fastest Growing Apps This Year.* http://mashable.com/2013/10/21/fastest-growing-apps/, Oktober 2013

[29] McAfee: *McAfee Safeguards Facebook Photos With McAfee Social Protection.* http://www.mcafee.com/us/about/news/2012/q3/20120828-01.aspx, August 2012

[30] Netzpolitik (Meister, A.): *Willst du einen Kredit? Aber nur, wenn uns deine Facebook-Freunde passen und du uns in deinen PayPal Account lässt.* https://netzpolitik.org/2013/willst-du-einen-kredit-aber-nur-wenn-uns-deine-facebook-freunde-passen-und-du-uns-in-deinen-paypal-account-laesst/, August 2013

[31] Office for National Statistics (UK): *Internet Access - Households and Individuals, 2013.* http://www.ons.gov.uk/ons/dcp171778_322713.pdf, August 2013

[32] ONVAB.com: *The Business of Facebook: Facts, Users Statistics & Their Usage Trends.* https://web.archive.org/web/20130921062126/http://onvab.com/blog/facebook-users-statistics-usage-trends/, Oktober 2012

[33] Pew Internet & American Life Project: *Trend Data (Teens).* http://www.pewinternet.org/Static-Pages/Trend-Data-(Teens).aspx, September 2012

[34] Pew Internet & American Life Project: *Smartphone Ownership 2013.* http://www.pewinternet.org/Reports/2013/Smartphone-Ownership-2013.aspx, Juni 2013

[35] Pew Internet & American Life Project: *Trend Data (Adults).* http://www.pewinternet.org/Static-Pages/Trend-Data-(Adults).aspx, Mai 2013

[36] Pew Internet & American Life Project (Duggan, M. ; Smith, A.): *Cell Internet Use 2013.* http://pewinternet.org/Reports/2013/Cell-Internet.aspx, September 2013

[37] Pew Internet & American Life Project (Zickuhr, K.): *Three-quarters of smartphone owners use location-based services.* http://www.pewinternet.org/Reports/2012/Location-based-services.aspx, Mai 2012

[38] PleaseRobMe.com: *Please Rob Me — Raising awareness about over-sharing.* http://pleaserobme.com/, Februar 2010

[39] ReadWrite (Lardinois, F.): *Creative Commons Releases Facebook App: Choose a License for Your Photos, Videos, and Status Updates.* http://readwrite.com/2009/05/18/creative_commons_releases_facebook_app, Mai 2009

[40] Spiegel Online: *Großversuch in den USA: Online-Daten verraten Versicherern Risikokunden.* http://www.spiegel.de/wirtschaft/service/grossversuch-in-den-usa-online-daten-verraten-versicherern-risikokunden-a-730062.html, November 2010

[41] Statistisches Bundesamt: *Private Haushalte in der Informationsgesellschaft (IKT) – Fachserie 15 Reihe 4 – 2012.* https://www.destatis.de/DE/Publikationen/Thematisch/EinkommenKonsumLebensbedingungen/PrivateHaushalte/PrivateHaushalteIKT2150400127004.pdf, März 2013

[42] Strategy Analytics: *Marktanteile der führenden Betriebssysteme am Absatz von Tablets weltweit vom 2. Quartal 2010 bis zum 1. Quartal 2013.* http://de.statista.com/statistik/daten/studie/196140/umfrage/marktanteile-der-fuehrenden-betriebssysteme-im-tablet-markt-seit-2010/, April 2013

[43] T3N.de (Petereit, D.): *Schlimmer als Apple: Android speichert Deine(!) Location auf Schritt und Tritt.* http://t3n.de/news/schlimmer-apple-android-speichert-deine-location-307050/, April 2011

[44] TechCrunch (Constine, J.): *Turkey Day Was Instagram's Busiest Ever, With 10 Million+ Thanksgiving Photos Shared At Up To 226 Per Second.* http://techcrunch.com/2012/11/23/instagram-thanksgiving/, November 2012

[45] TechCrunch (Moore, Robert J.): *Instagram Now Adding 130,000 Users Per Week: Analysis.* http://techcrunch.com/2011/03/10/instagram-adding-130000-users-per-week/, März 2011

[46] The New York Observer: Betabeat (Jeffries, A.): *As Banks Start Nosing Around Facebook and Twitter, the Wrong Friends Might Just Sink Your Credit.* http://betabeat.com/2011/12/as-banks-start-nosing-around-facebook-and-twitter-the-wrong-friends-might-just-sink-your-credit/, Dezember 2011

[47] The Telegraph (Evans, R.): *Using Facebook or Twitter 'could raise your insurance premiums by 10pc'.* http://www.telegraph.co.uk/finance/personalfinance/insurance/7269543/Using-Facebook-or-Twitter-could-raise-your-insurance-premiums-by-10pc.html, Februar 2010

[48] The Washington Times: *Face it: 'Book' no secret to employers.* http://www.washingtontimes.com/news/2006/jul/17/20060717-124952-1800r/, Juli 2006

[49] Tomorrow Focus AG: *Mobile Effects 2013-2.* http://de.slideshare.net/tomorrowfocus/mobile-effects-2013-2, Seite 19, Mai 2013

[50] Universität des Saarlandes (Backes, M.): *X-pire! - Wie man dem Internet das "Vergessen" beibringt.* https://www.infsec.cs.uni-saarland.de/projects/forgetful-internet/, Januar 2011

[51] XDA Developers (user CollegeDev): *[APP+MOD][4.1.2+ |STOCK][IRC-CHANNEL][GPL] PDroid 2.0 [2013-05-16 v1.57.1].* http://forum.xda-developers.com/showthread.php?t=1923576, Oktober 2012

[52] Yahoo! Deutschland Presseportal: *Europäischer Fotowettbewerb für den Flickr-Kalender 2014 – Außergewöhnliche Street Photography gesucht.* http://yahoo.enpress.de/Pressemeldungen/Europaeischer-Fotowettbewerb-fuer-den-Flickr-Kalender-2014-Aussergewoehnliche-Street-Photography-gesucht-/3446, Oktober 2013

[53] Yahoo! Deutschland Presseportal: *Flickr grenzenlos: ein Terabyte Speicherplatz, ein neues Fotoerlebnis im Web & eine brandneue App für Android-Geräte.* http://yahoo.enpress.de/Pressemeldungen/Flickr-grenzenlos-ein-Terabyte-Speicherplatz-ein-neues-Fotoerlebnis-im-Web-eine-brandneue-App-fuer-Android-Geraete/3327, Mai 2013

[54] Zeit Online: *Chefs prüfen Bewerber in sozialen Netzwerken.* http://www.zeit.de/online/2009/35/Firmen-Bewerber-Internet, September 2009

[55] Zeit Online: *Was Vorratsdaten über uns verraten.* http://www.zeit.de/digital/datenschutz/2011-02/vorratsdaten-malte-spitz, Februar 2011

Technische Standards, Patente und Whitepapers

[56] Adobe Systems Incorporated: XMP Specification: Part 1, Data Model, Serialization, and Core Properties. Version: 2012. http://wwwimages.adobe.com/www.adobe.com/content/dam/Adobe/en/devnet/xmp/pdfs/cc-201306/XMPSpecificationPart1.pdf. 2012. – Standard

[57] Adobe Systems Incorporated: XMP Specification Part 2: Additional Properties. Version: 2012. http://wwwimages.adobe.com/www.adobe.com/content/dam/Adobe/en/devnet/xmp/pdfs/cc-201306/XMPSpecificationPart2.pdf. 2012. – Standard

[58] Adobe Systems Incorporated: XMP Specification Part 3: Storage in Files. Version: 2012. http://wwwimages.adobe.com/www.adobe.com/content/dam/Adobe/en/devnet/xmp/pdfs/cc-201306/XMPSpecificationPart3.pdf. 2012. – Standard

[59] Butterfield, D. ; Fake, C. ; Henderson-Begg, C. ; Mourachov, S.: *Interestingness ranking of media objects.* Oktober 2006. – US Patent App. 11/350,981

[60] Camera & Imaging Products Association (CIPA): Exif 2.3 metadata for XMP. Version: 2012. http://www.cipa.jp/std/documents/e/DC-010-2012_E.pdf. 2012. – Standard

[61] Facebook, Ericsson, Qualcomm: *Whitepaper: A Focus on Efficiency.* https://fbcdn-dragon-a.akamaihd.net/hphotos-ak-prn1/851575_520797877991079_393255490_n.pdf, September 2013

[62] International Press Telecommunication Council (IPTC) ; Newspaper Association of America (NAA): IPTC-NAA Information Interchange Model Version 4. Version: 1999. http://www.iptc.org/std/IIM/4.1/specification/IIMV4.1.pdf. 1999. – Standard

[63] International Press Telecommunications Council: "IPTC Core" Schema for XMP. Version 1.0. Revision 8. Version: 2005. http://www.iptc.org/std/Iptc4xmpCore/1.0/specification/Iptc4xmpCore_1.0-spec-XMPSchema_8.pdf. 2005. – Standard

[64] International Press Telecommunications Council: IPTC Standard Photo Metadata. Version: Juli 2010. http://www.iptc.org/std/photometadata/specification/IPTC-PhotoMetadata-201007_1.pdf. 2010. – Standard

[65] Japan Electronics and Information Technology Industries Association: Exchangeable image file format for digital still cameras: Exif Version 2.3. Version: Mai 2013. http://www.jeita.or.jp/japanese/standard/book/CP-3451C_E. 2013 (JEITA CP-3451C). – Standard

[66] Metadata Working Group: *Guidelines for Handling Image Metadata. Version 2.0*. http://www.metadataworkinggroup.org/pdf/mwg_guidance.pdf, November 2010

[67] MSDN Library: *People Tagging Overview*. http://msdn.microsoft.com/en-us/library/ee719905(v=VS.85).aspx, July 2011

[68] NISO: *Understanding metadata*. National Information Standards Organization, 2004. http://www.niso.org/standards/resources/UnderstandingMetadata.pdf. – ISBN 1-880124-62-9

[69] Yahoo! Developer Network: *Yahoo! GeoPlanet Guide – Key concepts*. http://developer.yahoo.com/geo/geoplanet/guide/concepts.html,

Wissenschaftliche Veröffentlichungen

[70] Acquisti, Alessandro ; Gross, Ralph: Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. Version: 2006. In: Danezis, G. (Hrsg.) ; Golle, P. (Hrsg.): *Privacy Enhancing Technologies* Bd. 4258. Springer, 2006 (LNCS). – DOI 10.1007/11957454_3. – ISBN 978–3–540–68790–0, S. 36–58

[71] Ahern, Shane ; Eckles, Dean ; Good, Nathaniel S. ; King, Simon ; Naaman, Mor ; Nair, Rahul: Over-exposed?: Privacy Patterns and Considerations in Online and Mobile Photo Sharing. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, 2007 (CHI). – DOI 10.1145/1240624.1240683. – ISBN 978–1–59593–593–9, S. 357–366

[72] Ardagna, Claudio A. ; Cremonini, Marco ; De Capitani di Vimercati, Sabrina ; Samarati, Pierangela: An Obfuscation-Based Approach for Protecting Location Privacy. In: *Dependable and Secure Computing, IEEE Transactions on* 8 (2011), Jan, Nr. 1, S. 13–27. – DOI 10.1109/TDSC.2009.25. – ISSN 1545–5971

[73] Bartnik, Marcel: *Der Bildnisschutz im deutschen und französischen Zivilrecht*. Mohr Siebeck, 2004 (Studien zum ausländischen und internationalen Privatrecht). – ISBN 978–3–1614–8383–7

[74] Beede, Rodney ; Warbritton, Donald ; Han, Richard: MyShield: Protecting Mobile Device Data via Security Circles / Department of Computer Science, University of Colorado Boulder. 2012 (CU-CS-1091-12). – Technical Report

[75] Benisch, Michael ; Kelley, Patrick G. ; Sadeh, Norman ; Cranor, Lorrie F.: Capturing Location-privacy Preferences: Quantifying Accuracy and User-burden Tradeoffs. In: *Personal Ubiquitous Computing* 15 (2011), Oktober, Nr. 7, S. 679–694. – DOI 10.1007/s00779–010–0346–0. – ISSN 1617–4909

[76] Beresford, Alastair R. ; Rice, Andrew ; Skehin, Nicholas ; Sohan, Ripduman: MockDroid: Trading Privacy for Application Functionality on Smartphones. In: *Proceedings of the 12th Workshop on Mobile Computing Systems and Applications*, ACM, 2011 (HotMobile). – DOI 10.1145/2184489.2184500. – ISBN 978–1–4503–0649–2, S. 49–54

[77] Besmer, Andrew ; Lipford, Heather: Tagged Photos: Concerns, Perceptions, and Protections. In: *CHI '09 Extended Abstracts on Human Factors in Computing Systems*, ACM, 2009 (CHI EA). – DOI 10.1145/1520340.1520704. – ISBN 978–1–60558–247–4, S. 4585–4590

[78] Besmer, Andrew ; Richter Lipford, Heather: Moving Beyond Untagging: Photo Privacy in a Tagged World. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, 2010 (CHI). – DOI 10.1145/1753326.1753560. – ISBN 978–1–60558–929–9, S. 1563–1572

[79] Brooke, John: SUS: A quick and dirty usability scale. In: Jordan, P. W. (Hrsg.) ; Weerdmeester, B. (Hrsg.) ; Thomas, A. (Hrsg.) ; Mclelland, I. L. (Hrsg.): *Usability evaluation in industry*. London : Taylor and Francis, 1996, S. 189–194

[80] Brush, A.J. B. ; Krumm, John ; Scott, James: Exploring End User Preferences for Location Obfuscation, Location-based Services, and the Value of Location. In: *Proceedings of the 12th ACM International Conference on Ubiquitous Computing*, ACM, 2010 (Ubicomp). – DOI 10.1145/1864349.1864381. – ISBN 978–1–60558–843–8, S. 95–104

[81] Bulygin, Yuriy: Epidemics of Mobile Worms. In: *Performance, Computing, and Communications Conference*, IEEE, April 2007 (IPCCC). – DOI 10.1109/PCCC.2007.358929. – ISSN 1097–2641, S. 475–478

[82] Burghardt, Thorben ; Walter, Andreas. ; Buchmann, Erik ; Böhm, Klemens: PRIMO - Towards Privacy Aware Image Sharing. In: *IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology* Bd. 3, 2008 (WI-IAT). – DOI 10.1109/WIIAT.2008.23, S. 21–24

[83] Cetto, Alexandra ; Netter, Michael ; Pernul, Günther ; Richthammer, Christian ; Riesner, Moritz ; Roth, Christian ; Sänger, Johannes: Friend Inspector: A Serious Game to Enhance Privacy Awareness in Social Networks. In: *Proceedings of 2nd International Workshop on Intelligent Digital Games for Empowerment and Inclusion*, 2013 (IDGEI)

[84] Consolvo, Sunny ; Smith, Ian E. ; Matthews, Tara ; LaMarca, Anthony ; Tabert, Jason ; Powledge, Pauline: Location Disclosure to Social Relations: Why, when, & What People Want to Share. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, 2005 (CHI). – DOI 10.1145/1054972.1054985. – ISBN 1–58113–998–5, S. 81–90

[85] Cranor, Lorrie F.: Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice. In: *JTHTL* 10 (2012), Nr. 2, S. 273–308

[86] Cranor, Lorrie F. ; Arjula, Manjula ; Guduru, Praveen: Use of a P3P User Agent by Early Adopters. In: *Proceedings of the 2002 ACM Workshop on Privacy in the Electronic Society*, ACM, 2002 (WPES). – DOI 10.1145/644527.644528. – ISBN 1–58113–633–1, S. 1–10

[87] DeCew, Judith: Privacy. Version: Herbst 2013. `http://plato.stanford.edu/archives/fall2013/entries/privacy/`. In: Zalta, Edward N. (Hrsg.): *The Stanford Encyclopedia of Philosophy*. Herbst 2013

[88] Dhamija, Rachna ; Tygar, J. D. ; Hearst, Marti: Why Phishing Works. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, 2006 (CHI). – DOI 10.1145/1124772.1124861. – ISBN 1–59593–372–7, S. 581–590

[89] Egelman, Serge ; Cranor, Lorrie F. ; Chowdhury, Abdur: An Analysis of P3P-enabled Web Sites Among Top-20 Search Results. In: *Proceedings of the 8th International Conference on Electronic Commerce*, ACM, 2006 (ICEC). – DOI 10.1145/1151454.1151492. – ISBN 1–59593–392–1, S. 197–207

[90] Egelman, Serge ; Cranor, Lorrie F. ; Hong, Jason: You'Ve Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, 2008 (CHI). – DOI 10.1145/1357054.1357219. – ISBN 978–1–60558–011–1, S. 1065–1074

[91] Enck, William ; Gilbert, Peter ; Chun, Byung-Gon ; Cox, Landon P. ; Jung, Jaeyeon ; McDaniel, Patrick ; Sheth, Anmol N.: TaintDroid: An Information-flow Tracking System for Realtime Privacy Monitoring on Smartphones. In: *Proceedings of the 9th USENIX Conference on Operating Systems Design and Implementation*, USENIX Association, 2010 (OSDI), S. 1–15

[92] Fahl, Sascha ; Harbach, Marian ; Muders, Thomas ; Smith, Matthew: Confidentiality as a Service – Usable Security for the Cloud. In: *IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, 2012 (TrustCom). – DOI 10.1109/TrustCom.2012.112, S. 153–162

[93] Fahl, Sascha ; Harbach, Marian ; Muders, Thomas ; Smith, Matthew ; Sander, Uwe: Helping Johnny 2.0 to Encrypt His Facebook Conversations. In: *Proceedings of the Eighth Symposium on Usable Privacy and Security*, ACM, 2012 (SOUPS). – DOI 10.1145/2335356.2335371. – ISBN 978–1–4503–1532–6, S. 11:1–11:17

[94] Fasel, Ian R. ; Movellan, Javier R.: A Comparison of Face Detection Algorithms. In: *Proceedings of the International Conference on Artificial Neural Networks*, 2002 (ICANN). – DOI 10.1007/3–540–46084–5_214. – ISBN 3–540–44074–7, S. 1325–1332

[95] Fisher, Drew ; Dorner, Leah ; Wagner, David: Short Paper: Location Privacy: User Behavior in the Field. In: *Proceedings of the Second ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, ACM, 2012 (SPSM). – DOI 10.1145/2381934.2381945. – ISBN 978–1–4503–1666–8, S. 51–56

[96] Friedland, Gerald ; Sommer, Robin: Cybercasing the Joint: On the Privacy Implications of Geo-tagging. In: *Proceedings of the 5th USENIX Conference on Hot Topics in Security*, USENIX Association, 2010 (HotSec), S. 1–8

[97] Garfinkel, Simson L. ; Miller, Robert C.: Johnny 2: A User Test of Key Continuity Management with S/MIME and Outlook Express. In: *Proceedings of the 2005 Symposium on Usable Privacy and Security*, ACM, 2005 (SOUPS). – DOI 10.1145/1073001.1073003. – ISBN 1–59593–178–3, S. 13–24

[98] González, Marta C. ; Hidalgo, César A ; Barabási, Albert-László: Understanding individual human mobility patterns. In: *Nature* 453 (2008), Juni, Nr. 7196, S. 779–782. – DOI 10.1038/nature06958. – ISSN 1476–4687

[99] Gruteser, Marco ; Grunwald, Dirk: Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. In: *Proceedings of the 1st International Conference on Mobile Systems, Applications and Services*, ACM, 2003 (MobiSys). – DOI 10.1145/1066116.1189037, S. 31–42

[100] Henne, Benjamin ; Harbach, Marian ; Smith, Matthew: Location privacy revisited: factors of privacy decisions. In: *CHI '13 Extended Abstracts on Human Factors in Computing Systems*, ACM, 2013 (CHI EA). – DOI 10.1145/2468356.2468500. – ISBN 978–1–4503–1952–2, 805–810

[101] Henne, Benjamin ; Kater, Christian ; Smith, Matthew: On Usable Location Privacy for Android with Crowd-Recommendations. Version: 2014. In: Holz, T. (Hrsg.) ; Sotiris, I. (Hrsg.): *Trust and Trustworthy Computing* Bd. 8564. Springer, 2014 (LNCS). – DOI 10.1007/978–3–319–08593–7_5, S. 74–82

[102] Henne, Benjamin ; Kater, Christian ; Smith, Matthew ; Brenner, Michael: Selective cloaking: Need-to-know for location-based apps. In: *2013 Eleventh Annual International Conference on Privacy, Security and Trust*, 2013 (PST). – DOI 10.1109/PST.2013.6596032, S. 19–26

[103] Henne, Benjamin ; Koch, Maximilian ; Smith, Matthew: On the Awareness, Control and Privacy of Photo Metadata. In: Christin, N. (Hrsg.) ; Safavi-Naini, R. (Hrsg.): *Financial Cryptography and Data Security* Bd. 8437. Springer, 2014 (LNCS)

[104] Henne, Benjamin ; Linke, Marcel B. ; Smith, Matthew: A study on the Unawareness of Shared Photos in Social Network Services. In: *Proceedings of the IEEE Security and Privacy Workshop on Web 2.0 Security and Privacy*, IEEE, 2014 (W2SP '14)

[105] Henne, Benjamin ; Smith, Matthew: Awareness about Photos on the Web and How Privacy-Privacy-Tradeoffs Could Help. Version: 2013. In: Adams, A. A. (Hrsg.) ; Brenner, M. (Hrsg.) ; Smith, M. (Hrsg.): *FC 2013 Workshops, USEC and WAHC 2013, Okinawa, Japan, April 1, 2013, Revised Selected Papers* Bd. 7862. Springer, 2013 (LNCS). – DOI 10.1007/978–3–642–41320–9_9. – ISBN 978–3–642–41319–3, S. 131–148

[106] Henne, Benjamin ; Szongott, Christian ; Smith, Matthew: Towards a mobile security & privacy simulator. In: *2011 IEEE Conference on Open Systems*, IEEE, 2011 (ICOS). – DOI 10.1109/ICOS.2011.6079294, S. 95–100

[107] Henne, Benjamin ; Szongott, Christian ; Smith, Matthew: Coupled multi-agent simulations for mobile security & privacy research. In: *6th IEEE International Conference on Digital Ecosystems Technologies*, 2012 (DEST). – DOI 10.1109/DEST.2012.6227950. – ISSN 2150–4938, S. 48:1–48:6

[108] Henne, Benjamin ; Szongott, Christian ; Smith, Matthew: SnapMe if you can: privacy threats of other peoples' geo-tagged media and what we can do about it. In: *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks*, ACM, 2013 (WiSec). – DOI 10.1145/2462096.2462113. – ISBN 978–1–4503–1998–0, 95–106

[109] Holtz, Leif-Erik ; Nocun, Katharina ; Hansen, Marit: Towards Displaying Privacy Information with Icons. Version: 2011. In: Fischer-Hübner, S. (Hrsg.) ; Duquenoy, P. (Hrsg.) ; Hansen, M. (Hrsg.) ; Leenes, R. (Hrsg.) ; Zhang, G. (Hrsg.): *Privacy and Identity Management for Life* Bd. 352. Springer Berlin Heidelberg, 2011 (IFIP Advances in Information and Communication Technology). – DOI 10.1007/978–3–642–20769–3_27. – ISBN 978–3–642–20768–6, S. 338–348

[110] Hornyack, Peter ; Han, Seungyeop ; Jung, Jaeyeon ; Schechter, Stuart ; Wetherall, David: 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, 2011 (CCS). – DOI 10.1145/2046707.2046780. – ISBN 978–1–4503–0948–6, S. 639–652

[111] Iachello, Giovanni ; Hong, Jason: End-user Privacy in Human-computer Interaction. In: *Found. Trends Hum.-Comput. Interact.* 1 (2007), Januar, Nr. 1, S. 1–137. – DOI 10.1561/1100000004. – ISSN 1551–3955

[112] Iannella, Renato ; Finden, Adam: Privacy Awareness: Icons and Expression for Social Networks. In: *8th International Workshop for Technical, Economic and Legal Aspects of Business Models for Virtual Goods incorporating the 6th International ODRL Workshop*, 2009 (VirtualGoods)

[113] Johnson, Maritza ; Egelman, Serge ; Bellovin, Steven M.: Facebook and Privacy: It's Complicated. In: *Proceedings of the Eighth Symposium on Usable Privacy and Security*, ACM, 2012 (SOUPS). – DOI 10.1145/2335356.2335369. – ISBN 978–1–4503–1532–6, S. 9:1–9:15

[114] Kagal, Lalana ; Abelson, Hal: Access control is an inadequate framework for privacy protection. In: *W3C Privacy Workshop*, 2010

[115] Kang, Ted ; Kagal, Lalana: Enabling Privacy-Awareness in Social Networks. In: *AAAI Spring Symposium: Intelligent Information Privacy Management*, AAAI, 2010

[116] Kido, Hidetoshi ; Yanagisawa, Yutaka ; Satoh, Tetsuji: An anonymous communication technique using dummies for location-based services. In: *International Conference on Pervasive Services*, 2005 (ICPS). – DOI 10.1109/PERSER.2005.1506394, S. 88–97

[117] Klemperer, Peter ; Liang, Yuan ; Mazurek, Michelle ; Sleeper, Manya ; Ur, Blase ; Bauer, Lujo ; Cranor, Lorrie F. ; Gupta, Nitin ; Reiter, Michael: Tag, You Can See It!: Using Tags for Access Control in Photo Sharing. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, 2012 (CHI). – DOI 10.1145/2207676.2207728. – ISBN 978–1–4503–1015–4, S. 377–386

[118] Könings, Bastian ; Schaub, Florian ; Weber, Michael: Who, how, and why? Enhancing privacy awareness in Ubiquitous Computing. In: *2013 IEEE International Conference on Pervasive Computing and Communications Workshops*, 2013 (PERCOM Workshops). – DOI 10.1109/PerComW.2013.6529517, S. 364–367

[119] Krumm, John: A Survey of Computational Location Privacy. In: *Personal and Ubiquitous Computing* 13 (2009), August, Nr. 6, S. 391–399. – DOI 10.1007/s00779–008–0212–5. – ISSN 1617–4909

[120] Kumaraguru, Ponnurangam ; Cranor, Lorrie F.: Privacy Indexes: A Survey of Westin's Studies / Carnegie Mellon University. 2005 (CMU-ISRI-05-138). – ISRI Technical Report

[121] Lampinen, Airi ; Lehtinen, Vilma ; Lehmuskallio, Asko ; Tamminen, Sakari: We'Re in It Together: Interpersonal Management of Disclosure in Social Network Services. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, 2011 (CHI). – DOI 10.1145/1978942.1979420. – ISBN 978–1–4503–0228–9, S. 3217–3226

[122] Lin, Jialiu ; Amini, Shahriyar ; Hong, Jason I. ; Sadeh, Norman ; Lindqvist, Janne ; Zhang, Joy: Expectation and Purpose: Understanding Users' Mental Models of Mobile App Privacy Through Crowdsourcing. In: *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, ACM, 2012 (UbiComp). – DOI 10.1145/2370216.2370290. – ISBN 978–1–4503–1224–0, S. 501–510

[123] Liu, Yabing ; Gummadi, Krishna P. ; Krishnamurthy, Balachander ; Mislove, Alan: Analyzing Facebook Privacy Settings: User Expectations vs. Reality. In: *2011 ACM SIGCOMM Conference on Internet Measurement Conference*, ACM, 2011 (IMC). – DOI 10.1145/2068816.2068823. – ISBN 978–1–4503–1013–0, S. 61–70

[124] Mahmood, Shah ; Desmedt, Yvo: Usable Privacy by Visual and Interactive Control of Information Flow. Version: 2012. In: *Proceedings of the 20th International Conference on Security Protocols* Bd. 7622. Springer-Verlag, 2012 (LNCS). – DOI 10.1007/978–3–642–35694–0_20. – ISBN 978–3–642–35693–3, S. 181–188

[125] Malandrino, Delfina ; Petta, Andrea ; Scarano, Vittorio ; Serra, Luigi ; Spinelli, Raffaele ; Krishnamurthy, Balachander: Privacy Awareness About Information Leakage: Who Knows What About Me? In: *Proceedings of the 12th ACM Workshop on Workshop on Privacy in the Electronic Society*, ACM, 2013 (WPES). – DOI 10.1145/2517840.2517868. – ISBN 978–1–4503–2485–4, S. 279–284

[126] Mascetti, Sergio ; Freni, Dario ; Bettini, Claudio ; Wang, X. S. ; Jajodia, Sushil ; Milano, Università Di: On the Impact of User Movement Simulations in the Evaluation of LBS Privacy-Preserving Techniques. In: *Proceedings of the 1st International Workshop on Privacy in Location-Based Applications*, 2008

[127] Maurer, Max-Emanuel ; De Luca, Alexander ; Kempe, Sylvia: Using data type based security alert dialogs to raise online security awareness. In: *Proceedings of the Seventh Symposium on Usable Privacy and Security*, ACM, 2011 (SOUPS). – DOI 10.1145/2078827.2078830. – ISBN 978–1–4503–0911–0, S. 2:1–2:13

[128] Montjoye, Yves-Alexandre de ; Hidalgo, Cesar A. ; Verleysen, Michel ; Blondel, Vincent D.: Unique in the Crowd: The privacy bounds of human mobility. In: *Scientific Reports (nature.com)* 3 (2013). – DOI 10.1038/srep01376

[129] Phillips, P. J. ; Scruggs, W. T. ; O'Toole, Alice J. ; Flynn, Patrick J. ; Bowyer, Kevin W. ; Schott, Cathy L. ; Sharpe, Matthew: FRVT 2006 and ICE 2006 Large-Scale Results / NIST. Version: 2007. `http://www.face-rec.org/vendors/frvt2006andice2006largescalereport.pdf`. 2007. (NISTIR). – Bericht

[130] Porter Felt, Adrienne ; Egelman, Serge ; Wagner, David: I'Ve Got 99 Problems, but Vibration Ain'T One: A Survey of Smartphone Users' Concerns. In: *Proceedings of the Second ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, ACM, 2012 (SPSM). – DOI 10.1145/2381934.2381943. – ISBN 978–1–4503–1666–8, S. 33–44

[131] Pötzsch, Stefanie: Privacy Awareness: A Means to Solve the Privacy Paradox? Version: 2009. In: Matyáš, V. (Hrsg.) ; Fischer-Hübner, S. (Hrsg.) ; Cvrček, D. (Hrsg.) ; Švenda, P. (Hrsg.): *The Future of Identity in the Information Society* Bd. 298. Springer, 2009 (IFIP Advances in Information and Communication Technology). – DOI 10.1007/978–3–642–03315–5_17. – ISBN 978–3–642–03314–8, S. 226–236

[132] Schechter, Stuart E. ; Dhamija, Rachna. ; Ozment, Andy ; Fischer, Ian: The Emperor's New Security Indicators. In: *IEEE Symposium on Security and Privacy*, 2007 (SP). – DOI 10.1109/SP.2007.35. – ISSN 1081–6011, S. 51–65

[133] Sheng, Steve ; Broderick, Levi ; Koranda, Colleen A. ; Hyland, Jeremy J.: Why Johnny still can't encrypt: evaluating the usability of email encryption software. In: *Symposium On Usable Privacy and Security*, 2006 (SOUPS)

[134] Shin, Dongwan ; Lopes, Rodrigo: An Empirical Study of Visual Security Cues to Prevent the SSLstripping Attack. In: *Proceedings of the 27th Annual Computer Security Applications Conference*, ACM, 2011 (ACSAC). – DOI 10.1145/2076732.2076773. – ISBN 978–1–4503–0672–0, S. 287–296

[135] Smith, Matthew ; Henne, Benjamin ; Szongott, Christian ; Voigt, Gabriele von: Big data privacy issues in public social media. In: *6th IEEE International Conference on Digital Ecosystems Technologies*, 2012 (DEST). – DOI 10.1109/DEST.2012.6227909. – ISSN 2150–4938, S. 7:1–7:6

[136] Squicciarini, Anna C. ; Xu, Heng ; Zhang, Xiaolong: CoPE: Enabling Collaborative Privacy Management in Online Social Networks. In: *J. Am. Soc. Inf. Sci. Technol.* 62 (2011), März, Nr. 3, S. 521–534. – DOI 10.1002/asi.21473. – ISSN 1532–2882

[137] Srivatsa, Mudhakar ; Hicks, Mike: Deanonymizing Mobility Traces: Using Social Network As a Side-channel. In: *Proceedings of the 2012 ACM Conference on Computer and Communications Security*. New York, NY, USA : ACM, 2012 (CCS). – DOI 10.1145/2382196.2382262. – ISBN 978–1–4503–1651–4, 628–637

[138] Strater, Katherine ; Lipford, Heather R.: Strategies and Struggles with Privacy in an Online Social Networking Community. In: *Proceedings of the 22Nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction - Volume 1*, British Computer Society, 2008 (BCS-HCI). – ISBN 978–1–906124–04–5, S. 111–119

[139] Szongott, Christian ; Henne, Benjamin ; Smith, Matthew: Evaluating the threat of epidemic mobile malware. In: *8th International Conference on Wireless and Mobile Computing, Networking and Communications*, IEEE, 2012 (WiMob). – DOI 10.1109/WiMOB.2012.6379111. – ISSN 2160–4886, S. 443–450

[140] Szongott, Christian ; Henne, Benjamin ; Smith, Matthew: Mobile Evil Twin Malnets – The Worst of Both Worlds. Version: 2012. In: Pieprzyk, J. (Hrsg.) ; Sadeghi, A.-R. (Hrsg.) ; Manulis, M. (Hrsg.): *Cryptology and Network Security* Bd. 7712. Springer, 2012 (LNCS). – DOI 10.1007/978–3–642–35404–5_11. – ISBN 978–3–642–35403–8, S. 126–141

[141] Tang, Karen ; Hong, Jason ; Siewiorek, Dan: The Implications of Offering More Disclosure Choices for Social Location Sharing. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, 2012 (CHI). – DOI 10.1145/2207676.2207730. – ISBN 978–1–4503–1015–4, S. 391–394

[142] Tsai, Janice Y. ; Kelley, Patrick G. ; Cranor, Lorrie F. ; Sadeh, Norman: Location-sharing technologies: Privacy risks and controls. In: *37th Research Conference on Communication, Information and Internet Policy*, 2009 (TPRC)

[143] Tuunainen, Virpi K. ; Pitkänen, Olli ; ; Hovi, Marjaana: Users' Awareness of Privacy on Online Social Networking Sites – Case Facebook. In: *22nd Bled eConference*, 2009

[144] Ur, Blase ; Kelley, Patrick G. ; Komanduri, Saranga ; Lee, Joel ; Maass, Michael ; Mazurek, Michelle L. ; Passaro, Timothy ; Shay, Richard ; Vidas, Timothy ; Bauer, Lujo ; Christin, Nicolas ; Cranor, Lorrie F.: How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation. In: *Proceedings of the 21st USENIX Conference on Security Symposium*, USENIX Association, 2012 (Security), S. 5–5

[145] Varshney, Lav R.: Identity Annotation in Photo Collections: A Survey / MIT Media Lab. 2008. – MAS 964: Special Topics in Media Technology: Camera Culture

[146] Wang, Yang ; Norcie, Gregory ; Cranor, Lorrie F.: Who is Concerned About What? A Study of American, Chinese and Indian Users' Privacy Concerns on Social Network Sites. Version: 2011. In: *Proceedings of the 4th International Conference on Trust and Trustworthy Computing*. Springer-Verlag, 2011 (LNCS). – DOI 10.1007/978–3–642–21599–5_11. – ISBN 978–3–642–21598–8, S. 146–153

[147] Warren, Samuel D. ; Brandeis, Louis D.: The Right to Privacy. In: *Harward Law Review* 4 (1890), December, Nr. 5, S. 193–220

[148] Westin, Alan F.: *Privacy and Freedom*. Bodley Head, 1970. – ISBN 978–0–37–001325–1

[149] Westin, Alan F. ; Harris Interactive (Hrsg.): *Privacy On and Off the Internet: What Consumers Want (Study No. 15229)*. Februar 2002

[150] Whitten, Alma: Making Security Usable / School of Computer Science, Carnegie Mellon University. 2004 (CMU-CS-04-135). – Dissertation

[151] Whitten, Alma ; Tygar, J. D.: Why Johnny Can'T Encrypt: A Usability Evaluation of PGP 5.0. In: *Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8*, USENIX Association, 1999 (SSYM)

[152] Wills, Craig E. ; Zeljkovic, Mihajlo: A Personalized Approach to Web Privacy - Awareness, Attitudes and Actions. In: *Information Management & Computer Security* 19 (2011), Nr. 1, S. 53–73. – DOI 10.1108/09685221111115863

[153] Xu, Toby ; Cai, Ying: Feeling-based Location Privacy Protection for Location-based Services. In: *Proceedings of the 16th ACM Conference on Computer and Communications Security*, ACM, 2009 (CCS). – DOI 10.1145/1653662.1653704. – ISBN 978–1–60558–894–0, S. 348–357

[154] Zerr, Sergej ; Siersdorfer, Stefan ; Hare, Jonathon: PicAlert!: A System for Privacy-aware Image Classification and Retrieval. In: *Proceedings of the 21st ACM International Conference on Information and Knowledge Management*, ACM, 2012 (CIKM). – DOI 10.1145/2396761.2398735. – ISBN 978–1–4503–1156–4, S. 2710–2712

[155] Zerr, Sergej ; Siersdorfer, Stefan ; Hare, Jonathon ; Demidova, Elena: Privacy-aware Image Classification and Search. In: *Proceedings of the 35th International ACM SIGIR Conference on Research and Development in Information Retrieval*, ACM, 2012 (SIGIR). – DOI 10.1145/2348283.2348292. – ISBN 978–1–4503–1472–5, S. 35–44

Vom Autor betreute studentische Arbeiten

[156] Kater, Christian: *Ein Location-Privacy-Framework für Android*, Distributed Computing & Security Group, Institut für Verteilte Systeme, Leibniz Universität Hannover, Bachelorarbeit, Februar 2013

[157] Koch, Maximilian: *Eine Browser-Erweiterung zur Erhöhung der Transparenz und der Sicherheit von Foto-Metadaten im Web*, Distributed Computing & Security Group, Institut für Verteilte Systeme, Leibniz Universität Hannover, Bachelorarbeit, Februar 2013

[158] Linke, Marcel B.: *Analyse und Erweiterung eines Frameworks zur Modellierung von Nutzer-Bewegungen*, Distributed Computing & Security Group, Institut für Verteilte Systeme, Leibniz Universität Hannover, Bachelorarbeit, Juli 2010

[159] Protsch, Carsten: *Generalisierung und Anreicherung von Geodaten für den Mobile Security & Privacy Simulator*, Distributed Computing & Security Group, Institut für Verteilte Systeme, Leibniz Universität Hannover, Bachelorarbeit, September 2011

[160] Tute, Philipp: *Mechanismen zum Schutz der Privatsphäre in mobilen kontextabhängigen Informationssystemen*, Distributed Computing & Security Group, Institut für Verteilte Systeme, Leibniz Universität Hannover, Bachelorarbeit, September 2010

Lebenslauf

Benjamin Henne
geboren 1981 in Hannover

Akademischer Werdegang

06/2008 – heute	**Promotionsstudium** (Informatik), Leibniz Universität Hannover.
10/2005 – 06/2008	**Master of Science** (Informatik), Leibniz Universität Hannover. Masterarbeit: Workflows und Metascheduling im Grid-Computing
10/2002 – 11/2005	**Bachelor of Science** (Informatik), Universität Hannover. Bachelorarbeit: Aufbau eines IPSec-Testnetzes mit Einsatz einer PKI und OCSP

Schulische Ausbildung

06/2001	**Abitur**, Gymnasium Lehrte.

Beruflicher Werdegang

06/2008 – 06/2014	**Wissenschaftlicher Mitarbeiter**, Forschungszentrum L3S, Lehrgebiet Rechnernetze / Distributed Computing & Security Group, Fachgebiet Distributed Virtual Reality, Institut für Verteilte Systeme, Leibniz Universität Hannover. Projekte: • Kooperation mit IT.Niedersachsen • NTH Focused Research School IT-Ökosysteme • BMBF-gefördertes Projekt SLA4D-Grid • BMBF-gefördertes Projekt DGI-2 (Fachgebiet Sicherheit) Lehre: Konzeption und Durchführung von Übungen zu Security Engineering, Seminar: Aspekte Verteilter Systeme, Interdisziplinäres Seminar: Sicherheit und Privatsphäre in der Gesellschaft, Projekt: Sicherheit in Verteilten Systemen. Vorlesungsvertretung. Betreuung studentischer Abschlussarbeiten.
10/2006 – 09/2007	**Wissenschaftliche Hilfskraft**, Fachgebiet Software Engineering, Leibniz Universität Hannover. Betreuung von Netzwerk und Server-Systemen
04/2006 – 09/2007	**Wissenschaftliche Hilfskraft**, Regionales Rechenzentrum für Niedersachsen, Leibniz Universität Hannover. Grid-Computing und Netzwerk-Monitoring

08/2004 – 09/2004	**Praktikum**, GAD eG, Lehrte. Softwareentwicklung für Banken
01/2004 – 09/2006	**Studentische Hilfskraft**, Fachgebiet Software Engineering, Universität Hannover. Planung, Installation und Betreuung der IT-Infrastruktur

Auszeichnungen und zusätzliche Qualifikationen

10/2012 – 06/2013	**Promotion plus$^+$ qualifiziert**, Graduiertenakademie, Leibniz Universität Hannover. Promotionsbegleitenden Programm zur Führungskräfteentwicklung gefördert durch den Europäischen Fonds für Regionale Entwicklung
19.06.2012	**Student Scholarship**, IEEE Industrial Electronics Society. 6$^{\text{th}}$ IEEE International Conference on Digital Ecosystem Technologies (DEST 2012)
07.12.2007	**Ehrung**, Fakultät für Elektrotechnik und Informatik, Universität Hannover. Langjährige ehrenamtliche Tätigkeiten in der studentischen Selbstverwaltung: Vorsitz Fachschaftsrat, Vertreter Studienkommission, Schaffung eines Lernraumes, Erstsemester-Einführungen
06.11.2007	**Wissenschaftspreis Niedersachsen 2007**, Niedersächsisches Ministerium für Wissenschaft und Kultur Kategorie III: Studierende mit sehr guten Studienleistungen und zusätzlichem besonderen Engagement oder Leistungen in den Bereichen Familie, Ehrenamt, Musik oder Sport